ORDER

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

1600.68

DRAFT
(03/05/99)

SUBJECT: FEDERAL AVIATION ADMINISTRATION INFORMATION SYSTEMS SECURITY PROGRAM

A-WXYZ-2; A-FOF-0 (LTD)

FOREWARD

This order establishes comprehensive security policies for all information systems within the Federal Aviation Administration (FAA) and all information systems used on behalf of the FAA. Additionally, this order establishes information systems security (ISS) policies for FAA facilities and non-FAA facilities, such as contractor facilities.

With the publication of this order, delegation by the Administrator of DAA responsibility is to the head of each office that reports directly to the Administrator.

This order also streamlines the system security plan, certification and authorization processes to eliminate redundant efforts for system developers and operators.

This order establishes the security compliance review program for FAA facilities and risk assessment site surveys for non-FAA facilities, such as contractor facilities.

This order also establishes a security baseline of CS2 of the Common Criteria for new systems and establishes the requirement for risk management, including mitigation, for legacy systems.

It is intended that this order will provide high-level policy for FAA managers, employees and contractors to facilitate effective implementation and application of the provisions of this order.

We wish to thank the managers, employees and support contractors of the Federal Aviation Administration who participated in the development of this order.

Jane F. Garvey
Administrator

TABLE OF CONTENTS

Tables

CHAPTER 1. GENERAL OVERVIEW

1. PURPOSE. This Order establishes the Information Systems Security (ISS) Program, formerly known as the Automated Information Systems (AIS) Security Program. This Order designates program policy and objectives, establishes the ISS Organization, assigns responsibilities, and provides high level guidance to ensure that an appropriate level of Information Systems (IS) security is implemented throughout the FAA. It implements Department of Transportation ISS Policy (DOT H 1350.2), Departmental Information Resources Management Manual (DIRMM), Presidential Decision Directive #63, other statutory, regulatory, and Departmental policies and guidance (Appendix 2 provides a list of references) and generally accepted security and business practices.

2. DISTRIBUTION. This Order is distributed to the division level in Washington headquarters, regions, and centers with a limited distribution to all field offices and facilities.

3. CANCELLATION. This Order cancels FAA Order 1600.54B, FAA Automated Information Systems Security Handbook, except for Chapter 5 "Computer Processing of Classified Information", and cancels FAA Order 1600.66, Telecommunications and Information Systems Security Policy. References to these orders in existing contracts will be replaced with references to FAA Order 1600.68.

4. SCOPE. This Order applies to all legacy, current and future FAA information systems, including prototypes and telecommunications. It also applies to all FAA employees, contractors, and users of FAA information systems and information systems used for the FAA.

5. BACKGROUND. The Presidential Decision Directive (PDD #63), *Critical Infrastructure Protection*, dated May, 1998, states that each department and agency shall be responsible for protecting its' own critical infrastructure, especially its' cyber-based systems. Therefore, the FAA is responsible for ensuring that all of its information systems are protected from threats to integrity, availability, and confidentiality. The FAA maintains a variety of information systems that supports the agency, aviation safety and security, and the National Airspace System (NAS). The NAS and other FAA information systems depend on adequate ISS for proper operation. The increasing number of network-based attacks, the reliance on the Internet for quickly communicating information, and the vulnerability of information systems to exploitation by threat agents require FAA to apply a more rigorous risk management approach to its operational and administrative support systems.

6. PRECEDENCE AND INTERPRETATION. This Order has precedence over other FAA Orders that contain conflicting, incomplete or obsolete ISS policy, guidance or instruction. The Associate Administrator for Civil Aviation Security is authorized to interpret the provisions of this Order, resolve any apparent conflicts with other Orders, and modify this Order to be consistent with significant changes in Federal, departmental and FAA mandates.

7. EXPLANATION OF CHANGES. These changes reflect differences between FAA Order 1600.54B and this Order**.**

a. Standards and subject area guidance will be developed upon publication of this Order and maintained by ACS.

b. ***Designated Approving Authority (DAA):*** Delegation by the Administrator of DAA responsibility is to the Associate Administrator and the Director of each office that reports directly to the Administrator.

(1) Each DAA may delegate this authority in writing to a member of the SES.

(2) The DAA or designee must be at least one level above the individual responsible for developing or operating the information system (IS).

(3) The DAA or designee for a system must be selected from an organization representing the operational owner and/or data owners.

(4) Selection of the DAA or designee from the developer's organization represents a conflict of interest.

c. ***System Security Plan (SSP) Package:*** The SSP Package will replace the Sensitive Application Certification (SAC). This package is made up of the security plan, including risk assessment and security test results, certification and authorization.

(1) *Security Plan:* Provides an overview of ISS requirements and describes how and when those requirements are being met or will be met.

(2) *Certification:* The ISS Division (ACO-700) or the Certifying Authority (regional Security Divisions) will certify a system for security as documented in its SSP.

(3) *Authorization:* A written decision by the DAA to permit an information system to operate at an acceptable level of risk. The previous term was accreditation.

(4) *Interim Authorization:* The authority to operate may be granted for a fixed period of time, not to exceed 1 year, based on incomplete documentation, such as the security plan.

d. ***Acquisition Management System (AMS):*** Security activities that take place during the acquisition cycle are defined, including Screening Information Request (SIR), statements of work (SOW) and contracts.

e. ***Life Cycle Management:*** Security activities that take place during a system's life cycle are defined and cross-referenced from initiation of a system to decommissioning.

f. ***Baseline Security Levels:*** FAA information system security baseline is stated and based on the *Common Criteria* as described in NIST guidelines and in accordance with ICAO agreements.

g. ***Certification/Authorization Schedule:*** Beginning each fiscal year, a schedule for information system-wide certification and authorization shall be issued by each organization directly reporting to AOA-1 and a copy of the schedule shall be forwarded to the ISS Division.

h. ***Training:*** The ISS Division provides guidance (based on NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model)* to the lines of business in establishing ISS awareness, training and education. Training is role and performance-based, segmented into 6 functional areas:

(1) Manage,
(2) Acquire,
(3) Design and develop,
(4) Implement and operate,
(5) Review and evaluate,
(6) User.

i. ***FOUO/Sensitive Security Information (SSI):*** This order includes guidance for the appropriate handling of this type of information.

j. ***Security Compliance Reviews:*** Inspections that examine operational assurance whether the system is meeting stated or implied security requirements, including system and organizational policies stated in the SSP. The ISS Division (ACO-700) or the regional Security Divisions conduct the inspections.

(1) *Frequency:* Each system will be reauthorized every three years.

(2) *Systems:* All FAA information systems are subject to review.

(3) *Facilities:* All FAA facilities and non-FAA facilities where FAA information systems, or any portion of FAA information systems, will be developed, housed or operated, are subject to review.

k. ***Incident Reporting:*** Types of reported ISS security incidents are listed and an incident reporting structure chart is included. ISS notification structure to disseminate ISS alerts and information bulletins is defined with an accompanying chart.

8. POLICY. The FAA shall implement and maintain a program to ensure that adequate protection is provided for all information systems that collect, process, transmit, store, and/or disseminate information and shall meet all applicable federal statutes and regulations governing this area.

9. POLICY IMPLEMENTATION. The FAA shall:

a. Ensure that security needs and cost estimates are addressed in the acquisition management cycle for systems and services.

b. Require that each organization directly reporting to the Administrator (AOA-1) obtain formal security certification for its Information Systems (IS) from the Information Systems Security (ISS) Division in the Office of Civil Aviation Security Operations at FAA headquarters or a Certifying Authority (CA) designated by the ISS Division Manager.

c. Designated Approving Authority (DAA) is hereby delegated to each executive directly reporting to AOA-1 to authorize a system to process information in the performance of the FAA mission. The DAA is a senior management official who is empowered to authorize the processing of information systems for which that organization is responsible This authority may be further delegated no lower in the organization than to members of the Senior Executive Service (SES), provided delegation is in writing. However, approving authority must be limited to an official at least one level above the manager responsible for developing or operating an information system.

d. Require that the minimum documentation for authorizing an information system shall include the authorization statement, the certification report, the ISS plan, and operational and security system test results.

e. Develop ISS plans by using the controls specified in the Computer Security Act of 1987, OMB Circular A-130, DOT regulations, National Institute of Standards and Technology (NIST) guidelines and other statutory and regulatory policies and guidelines.

f. Require that all FAA personnel and contractor personnel working for, or on behalf of, the FAA take adequate measures to provide for:

(1) The accountability, availability, confidentiality, and integrity of information, data and source code.

(2) The protection of information and the information systems that store, process, or transmit this information.

g. Ensure that each organization directly reporting to AOA-1 has identified, inventoried, and reported to the manager of the ISS Division all information systems that are within its control and identify the security level of each system. This inventory must be updated on a biannual basis.

h. Conduct risk assessments that address vulnerabilities, threats, risk, safeguards and risk acceptance.

i. Reassess security controls periodically and, where feasible, test ISS plans.

j. Provide an adequate level of protection for the FAA's general support systems, major application systems, and the facilities for housing or supporting the operation of such systems.

10. RESPONSIBILITIES. Responsibility for the FAA Information System Security Program lies with the following officials:

a. Chief Information Officer (CIO)

The FAA's Chief Information Officer has the following ISS Program responsibilities (*CIO responsibilities will be updated as required)*:

(1) Develop a strategic Information Resources Management (IRM) five-year plan which incorporates a summary of computer security planning.

(2) Assure that information systems operation policies, procedures, and practices comply with this order.

(3) Oversee implementation of security awareness training for users of federal information systems.

b. Organizations Directly Reporting to AOA-1

These offices shall participate in formulation and approval of FAA Orders, requirements, procedures, and controls for the ISS program. They shall comply with these according to guidance issued by the Associate Administrator for Civil Aviation Security, ACS.

The head of each office is responsible for:

(1) Implement FAA ISS policy within the respective organization according to the requirements of this Order.

(2) Designate a Designated Approving Authority (DAA) and alternate who will be responsible for providing executive leadership and emphasis for their ISS program (See Table 1-1 of this Chapter).

(3) Ensure that security test and evaluation (ST&E) is conducted in accordance with Chapter 10 of this Order.

(4) Ensure that all information systems are identified and security level is designated appropriately.

(5) Ensure that all IS acquisition and contracting actions, including service life extension activities, comply with this Order.

(6) Ensure that IS security and contingency plans are developed for all information systems within the organization and that the plans apply the controls consistent with Section 3 of Appendix III to OMB Circular A-130.

(7) Ensure that security needs are addressed throughout the IS life cycle.

(8) Designate the position sensitivity level of employee and contractor positions associated with the management or operation of information systems.

(9) Ensure that personnel who occupy positions designated computer/ADP sensitive, shall be appropriately cleared and granted access prior to occupying such a position. Interim clearance and access may be authorized, where deemed necessary by the Investigations Division at Headquarters (ACO-300) or the SSE in Regions and Centers. Contractor personnel shall have appropriate clearances prior to commencing work in these positions.

(10) Ensure that the ISS awareness and training are incorporated in the policies and procedures for the organization.

(11) Ensure that budget requests for ISS improvements are reviewed by the ISS Division.

(12) Ensure that incidents are reported to the ISS Division in accordance with Chapter 11 of this Order.

(13) Provide resources necessary to develop and sustain the ISS program.

c. Designated Approving Authority

A Designated Approving Authority (DAA) is an FAA senior management official, appointed for each office directly reporting to AOA-1, with the following ISS responsibilities:

(1) Designate one Information Systems Security Manager (ISSM) and alternate who will be responsible for the development and management of the ISS Program for their organization. The ISSM

and alternate shall be identified in writing to the Office of Civil Aviation Security (ACS) (See Table 1-1 of this Chapter.)

(2) Identify the information category, IS security level and appropriate protection for information (See paragraph 203 of this Order).

(3) Authorize any information system within their line of business to operate or continue to operate and process any level of information in the performance of the FAA mission.

(4) Authorize interconnection among information systems, based upon the acceptance of risk to the system, prior to connecting with other systems. Where connection is authorized (includes interim authorization), controls shall be established which are consistent with the rules of the systems and in accordance with interconnection guidance published in this Order.

(5) Affirm that an information system meets all federal ISS policies, regulations, and standards and that the results of system tests, including security tests, demonstrate that the installed security safeguards provide adequate protection.

d. Information Systems Security Managers (ISSM)

ISSMs are responsible for the development and management of the ISS Program for an office directly reporting to AOA-1, as follows:

(1) Ensure that each information system is provided adequate protection commensurate with its security level.

(2) Designate in writing Information Systems Security Officers (ISSOs) in the Regions, Centers and Headquarters who will implement the ISS Program within their organization. See Table 1-1 of this Chapter). The ISSOs shall be identified to the Manager of the ISS Division at FAA headquarters and the appropriate servicing security element. There is no limit to the number of ISSOs within a line of business. It is recommended that a regional ISSO be designated to coordinate security activities.

(3) Ensure that an information system inventory is maintained. A copy of the system inventory shall be provided on a biannual basis to the servicing security element (SSE).

(4) Ensure that an IS security plan is developed and implemented for each IS.

(5) Compile inputs for the FAA annual ISS work plan for submission to the Manager of the ISS Division.

(6) Provide an annual summary of the organization's ISS Program implementation to the Manager of ISS Division.

(7) Ensure that a contingency plan is developed for each information system within their organization and that each contingency plan addresses emergency response, backup, and recovery actions required to provide reasonable continuity.

(8) Ensure that for each information system a management control process is established to assure administrative, physical and technical safeguards.

(9) Ensure that each new information system undergoes a review after testing and before implementation and is certified for security by the Manager of the ISS Division or other Certifying Authority (CA) designated by the ISS Division (See Table 1-1 of this Chapter).

(10) Ensure that each information system is reviewed as specified in paragraphs 242, 243 and 244.

(11) Assist the DAA in ensuring that each information will undergo detailed review leading to formal authorization.

(12) Ensure security testing and evaluation (ST&E) is conducted within the LOB in accordance with an approved ST&E plan and Chapter 10 of this Order.

(13) Ensure that each newly acquired information system has the minimum security functionality and assurance requirements as appropriate to its security level.

(14) Implement an ISS awareness and training process. This includes providing mandatory periodic training in ISS fundamentals and performance level training in security planning and management, ISS policies and procedures, contingency planning, and system life cycle management.

(15) Report and compile all incidents from the ISSOs to the DAA and the ISS Division according to Chapter 10 of this Order.

e. Information Systems Security Officers (ISSO)

ISSOs assist the organizational ISSM and alternate in implementing the ISS Program and have the following responsibilities:

(1) Plan, develop, and implement ISS safeguards within the areas of responsibility designated by the appropriate ISSM.

(2) Develop a contingency plan for each of their information systems which addresses emergency response, backup, and recovery actions required to provide reasonable continuity of data processing support should events occur that prevent normal operations.

(3) Maintain and, where feasible, periodically test contingency plans.

(4) Report and document all ISS incidents to the appropriate ISSM and the servicing security element (SSE) through the Information Systems Security Coordinator (ISSC) at Regions, Centers and Headquarters (See Table 1-1 of this Chapter).

(5) Compile an inventory of allocated information systems and provide a copy of the inventory on a biannual basis to the SSE and the ISSM.

(6) Coordinate the implementation of the line of business security awareness and training process with other ISSOs within the same line of business and with the ISSM.

f. Associate Administrator for Civil Aviation Security (ACS)

The Associate Administrator for Civil Aviation Security (ACS) has overall responsibility for the establishment and administration of the FAA ISS Program (See Table 1-1 of this Chapter). The ISS Program has distributed responsibilities that depend on the involvement of all FAA organizations which acquire, develop, operate, or replace information systems.

(1) Office of Civil Aviation Security Operations (ACO)

The Director of the Office of Civil Aviation Security Operations (ACO-1) has the following responsibilities, tasked to the Manager of the Information Systems Security Division (ACO-700) (See Table 1-1 of this Chapter):

(a) Advise the Associate Administrator for Civil Aviation Security, ACS-1, and FAA organizations concerning the FAA ISS Program.

(b) Administer the FAA ISS Program elements including information systems security policy formulation, enforcement, and awareness.

(c) Serve as the FAA ISS Certifying Authority (CA). The certification process includes initial review and approval of IS security requirements for compliance with federal law and policies and monitoring the IS throughout development and testing for compliance with ISS requirements.

(d) Develop and disseminate FAA ISS policies, plans, procedures, and standards.

(e) Compile and submit the FAA annual ISS work plan in accordance with OMB guidance.

(f) Oversee and assist with FAA implementation of, and compliance with, ISS aspects of federal laws, standards, and regulations.

(g) Represent the FAA on all matters pertaining to ISS.

(h) Review the budget requests for ISS improvements submitted by FAA organizations.

(i) Review ISS security plans, including ISS certification, and provide recommendations to the DAA concerning the associated risks.

(j) Ensure that there is an incident handling response capability to provide help to users when an ISS incident occurs in the FAA and assist the lines of business in pursuing appropriate legal action, consistent with Department of Justice, DOT and AGC guidance. Compile incident information for ISS program improvement and analyze for trends.

(k) Ensure that there is a capability to share information concerning common vulnerabilities and threats. This capability shall share information with other internal and external organizations, consistent with FAA and NIST policies and procedures.

(l) Provide ISS related information to the Information Systems Security Manager (ISSM) for each organization directly reporting to AOA-1 and coordinate the activities of Information Systems Security Coordinators (ISSCs) within the ACS organization.

(m) Review ISS awareness and technical training guidance and assist FAA organizations in meeting the requirements for this training as identified in NIST Special Publication 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model.*

(n) Foster compliance with various components of the ISS Program through security certification, awareness activities, and periodic information system reviews.

(o) Foster and measure compliance with the ISS policy and guidelines through substantive security evaluations.

(p) Maintain an inventory of information systems.

(q) Develop a schedule each fiscal year for performance of regional SSE program reviews and staff assistance visits (SAV) in accordance with FAA Order 1650.7 and Chapter 9 of this Order.

(r) Review security testing and evaluation (ST&E) plans for compliance with this Order and Federal law.

(2) Servicing Security Element (SSE)

The servicing security element at each FAA Region/Center has the following responsibilities (See Table 1-1 of this Chapter):

(a) Implement FAA ISS Program responsibilities within their region/center.

(b) Select an ISS Coordinator (ISSC) to perform duties consistent with the responsibilities specified in paragraph (3) below.

(c) Ensure that all ISS plans and authorization documentation for regional/center information systems are reviewed and make certification and accreditation recommendations to the ISS Division and the IS developers or owners.

(d) Ensure that there is a capability to share information concerning common ISS vulnerabilities and threats. This capability shall share information with other internal and external organizations on a need to know basis consistent with FAA, DOT, NIST, DOJ and other agency policies and procedures.

(e) Ensure that all ISS incidents are reported to the Manager of the ISS Division, documented, and, as appropriate, investigated.

(f) Investigate ISS incidents and assist regional/center management in pursuing appropriate legal action, consistent with Department of Justice and DOT and FAA policy.

(g) Provide an annual summary of ISS Program implementation within the region or center to the Manager of the ISS Division for each calendar year and submit by February 1 of the following year.

(h) Ensure that a copy of the system inventories received from ISSOs is provided on a biannual basis to the Manager of the ISS Division.

(i) Ensure development of a schedule of ISS inspections at FAA facilities and non-FAA facilities providing information system development or operations for the FAA, in accordance with FAA Order 1650.7 and Chapter 9 of this Order.

(j) Ensure that ST&E plans are reviewed for compliance with Chapter 9 of this Order. Coordinate with the ISS Division as part of the review process.

(3) Information Systems Security Coordinators (ISSC)

The Information Systems Security Coordinators (ISSCs) are employees of an SSE, which is the Security Division located at each region or center. ISSCs have the following ISS Program responsibilities (See Table 1-1 of this Chapter):

(a) Serve as the coordinator for all matters involving regional ISS plans and certification. This includes initial and final review of system security requirements for compliance with the law, as well as FAA and other relevant federal policies. This also includes reviewing information systems and inspecting facilities during development and upon commissioning for conformance with security plans and specifications.

(b) Review all ISS plans and authorization documentation for regional/center information systems and make certification and authorization recommendations to the ISS Division.

(c) Share information concerning common ISS vulnerabilities and threats with other internal and external organizations on a need to know basis consistent with FAA, DOT, NIST, DOJ and other agency policies and procedures.

(d) Document and report all ISS incidents to the manager of the SSE and the Manager of the ISS Division as quickly as possible. Coordinate with the ISSO for resolution of situations.

(e) Investigate, in coordination with the internal security investigations program, ISS incidents and assist regional/center management in pursuing appropriate legal action, consistent with Department of Justice and DOT guidance and FAA policy.

(f) Prepare an annual summary of ISS Program implementation within the region or center for submission to the manager of the SSE.

(g) Compile and review the inventory of allocated information systems from the ISSOs and provide a copy of the inventory on a biannual basis to the manager of the SSE (see paragraph 10d(3)).

(h) Conduct regional/center ISS security compliance reviews (inspections) and develop a schedule in accordance with FAA Order 1650.7 and Chapter 9 of this Order.

(i) Coordinate a regional/center ISS security training program with the ISSOs of the various lines of business in the Region or Center.

g. Contracting Officers (CO)

(1) CO shall ensure that ISS functional and assurance requirements are incorporated in IS procurement documents in accordance with this Order.

(2) CO shall ensure that the IS procurement documents are sent to the SSE for review.

(3) CO shall ensure that IS procurement documents state that this Order applies to all non-FAA facilities where FAA information systems, or any portion of FAA information systems, will be developed, housed or operated.

Table 1-1. ISS Organization (Refer to Figures 11-1 and 11-2 for Communications Flow)

Designated Approving Authority (DAA): *Associate Administrator of each line of business (LOB) and each office that reports directly to the Administrator*. The DAA responsibilities may be delegated in writing to a member of the Senior Executive Service (SES). The DAA must be selected from an organization representing the operational owner and/or the data owners. Selection of the DAA from the developer's organization represents a conflict of interest. The DAA must be at least one level above the individual responsible for developing or operating the information system. *The DAA designates an Information Systems Security Manager and alternate in writing to the ISS Division. The DAA coordinates with ACO-700 on all matters relating to ISS within the FAA.*	***Associate Administrator for Civil Aviation Security (ACS-1):*** *Overall responsibility for the establishment and administration of the FAA ISS Program.* ***Office of Civil Aviation Security Operations (ACO-1):*** *Ensures management and implementation of the ISS Program through the Information Systems Security Division (ACO-700).* *ACO-700 coordinates with the DAA on all matters relating to ISS within the FAA*
Information Systems Security Manager (ISSM): *One individual and an alternate responsible for development and management of the ISS Program within the organization and appointed by the DAA in writing.* The DAA may choose to designate an ISSM in each region and center to coordinate security activities for that region. *The ISSM designates the ISSOs in writing within each organization. The ISSM coordinates with the ISSD for all matters relating to ISS within their LOB and with the regional/center ISSOs.*	***Information Systems Security Division (ISSD) (ACO-700):*** *Manages and implements the ISS Program.* Serves as the Certifying Authority (CA) within the ISS certification process. A designee may be assigned in writing by the ISSD Manager (In a region/center, this is the Servicing Security Element (SSE) Manager). *The ISSD coordinates with ACS-1/ACO-1, the ISSMs and the SSE in each region/center. The ISSD coordinates the activities of the Information Systems Security Coordinators (ISSCs) at each region/center SSE.*
***Regional/Center LOB Management*:** See responsibilities for LOB/Each Office reporting directly to the Administrator (Chapter 1, paragraph 10b.) *Regional/Center LOB management coordinates with the SSE on all matters relating to ISS within their region/center.*	***Servicing Security Elements (SSE) (ACO-700, -700, ACT-8):*** *The Security Divisions are located at HQ, each region and center.* The SSE Manager is designated as the Certifying Authority in writing by the ISSD Manager when a local system is being developed. *The SSE and ISSD coordinate on all matters relating to ISS within their region/center. The SSE coordinates with the regional/center LOB management on all matters relating to ISS within their region/center. The ISSC is assigned to each HQ, region and center SSE.*
Information Systems Security Officer (ISSO): *Individuals designated in writing that assist the ISSM in implementing the ISS Program.* The ISSM may appoint as many as necessary within a LOB. (Designation of a regional/center ISSO as focal point for all information going to the ISSM and ISSC is recommended). *ISSOs coordinate with and report activities to Region/Center LOB management, ISSCs and ISSM on all matters relating to ISS within their region*	***Information Systems Security Coordinators (ISSC):*** *ACS employees assigned to SSE in HQ, each region and center.* They are the field focal point for information system security. *ISSCs coordinate with the regional/center ISSOs and are the liaison between the ISSD and the SSE.*

11. STATUTORY, POLICY AND REGULATORY MANDATES.

a. Computer Security Act. The Computer Security Act of 1987, Public Law 100-235, dated January 8, 1988, is the cornerstone of computer security within the Federal Government and has been used as a basis for the development of FAA policy. This order is consistent with the policies and guidance listed in Appendix 2. Public Law 100-235 requires Federal agencies to identify sensitive systems, provide security training, and develop and implement a security plan for each sensitive system. As the laws change, FAA will adjust its policy and directive guidance accordingly.

b. Policy Requirements.

(1) The **Office of Management and Budget** issues basic Federal policy for the security of information systems. OMB circulars for security include OMB Circular A-130, Appendix III, and OMB Circular A-123, Internal Control Systems. OMB Bulletins provide detailed security guidance.

(2) The **National Institute of Standards and Technology (NIST)** has the responsibility, as assigned by The Computer Security Act of 1987, for developing computer security standards and guidelines for Federal unclassified systems. Appendix 2 lists NIST's Federal Information Processing Standards (FIPS) and other publications applicable to ISS.

(3) The **Office of Personnel Management** (OPM) has the responsibility, as assigned by The Computer Security Act, to issue security training guidance. OPM also specifies the procedures for designating sensitive positions and screening incumbents as captured in FAA Order 1600.1. OMB Circular A-130, specifies training for all Federal employees who manage and use Federal computer systems that process U. S. Government information. Specific amounts, types, and intervals of security training are identified for Federal computer users, administrators, technicians, managers, and executives in A-130.

c. The **Presidential Decision Directive (PDD) #63, *Critical Infrastructure Protection (May 1998)***, builds on the recommendations of the Presidential Commission of Critical Infrastructure Protection (PCCIP). PDD #63 addresses the cyber and physical infrastructure vulnerabilities of the Federal government by requiring each Department and agency to work to reduce its exposure to new threats. PDD #63 also directs the FAA to develop and implement a comprehensive NAS security program to protect the modernized NAS from information-based and other disruptions and attacks.

12 - 199. RESERVED.

CHAPTER 2. CERTIFICATION AND AUTHORIZATION PROCESS

SECTION 1. OVERVIEW

200. PURPOSE.

a. FAA information systems must be given a level of protection commensurate with their importance to the overall Agency mission and with the mission risks introduced by using this information technology. The importance of the information system is based on both intangibles, such as the value of the information being processed and the functionality being provided, and tangibles, such as the value of physical facilities. Information systems will be placed into categories, each with its own unique management and security concerns.

b. Information system (IS) security levels are used to define the protection requirements for FAA information and information systems. Once information has been categorized, the appropriate IS security level for that information must be determined, so that protective measures can be applied. The purpose of this section is to provide guidance for determining IS security levels (see table 2-2).

201. RESPONSIBILITY. The DAA is responsible for identifying the category, IS security level, and appropriate protection for information; the owner of the information is responsible for appropriately marking the information according to its IS security level. When an information system is being developed, the developing system owner consults with the intended operational system owner to determine the appropriate security level and protection. For example, a new national Air Traffic Control system in development would be owned during development by the Administrator for Research and Acquisition, who would discuss security matters with the Air Traffic Services, the intended operational owner. All users of FAA information, including owners of information systems, are responsible for protecting information according to its sensitivity level.

202. ISS: THE SECURITY LIFE CYCLE PROCESS. This paragraph describes the ISS life-cycle process that applies to FAA systems. Life-cycle security refers to the fact that security must be considered continuously from the system's inception to its final disposition. Security requirements shall be identified and methods for compliance instituted early in the mission needs statement and extending through design, development (including prototypes), acquisition, deployment, operations, maintenance, and test. The ISSP covers security considerations up to and including the final disposition of the system being decommissioned or being listed as surplus property. Appropriate technical, administrative, physical, and personnel security requirements must be included in specifications for acquiring or operating information technology installations, equipment, software and related services whether procured or developed by the Agency or GSA. These security requirements shall be reviewed and approved by the DAA and the ISS Division or designee. Additional life-cycle security guidance is provided by OMB Circular A-130, OPM, and DOT in the DIRMM.

Life-cycle security is the process whereby each phase in the system's planning, development, and operation includes structured rules and checks to ensure that system security will be maintained. Involvement with security crosses all phases of a system life cycle. The phases of the System Development Life Cycle are Initiation, Definition, Design, Development, Test and Evaluation, Operation, and Decommissioning. During each phase, the ISSP addresses the security appropriate to that life-cycle phase. Security personnel must be involved in all phases of the system life cycle. Table 2-1 defines system security engineering efforts that shall be performed during each system life-cycle phase and provides references to the pertinent parts of this Order where these activities are addressed. Security activities throughout the life cycle contribute to developing and maintaining the ISS plan, to understanding and mitigating threats and vulnerabilities, to planning and carrying out secure system operations, and to safeguarding FAA assets.

Table 2-1. Overview of Life-Cycle Security Activities

Phase	Activities	References
Initiation	• Define security goals	Chapter 2, Section 2
	• Initiate system security plan	Chapter 2, Section 3
	• Initiate risk management program	Chapter 2, Section 4
	• Enact contingency/disaster recovery planning for system under development	Chapter 2, Section 7
	• Prepare security acquisition guidelines	Chapter 3
Definition	• Identify security policy and operational security constraints	Chapter 2, Section 4
	• Define security boundary	Chapter 2, Section 2
	• Identify sensitive data	Chapter 2, Section 3
	• Conduct risk assessment	Chapter 2, Section 4
	• Identify security requirements	Chapter 2 & Appendix 5
	• Identify sensitive processes	Chapter 2 & Appendix 5
	• Update system security plan	Chapter 2, Section3 Chapter 3
	• Prepare security input for system acquisition specifications	
Design	• Define security architecture consistent with system design	Chapter 2, Section 3
	• Define risk-based, cost-effective security mechanisms	Chapter 2, Section 4
	• Define security implementation standards and practices	Chapter 2, Section 4
	• Update system security plan	Chapter 2, Section 3
	• Prepare acquisition specifications for security components	Chapter 3 Chapter 2 Section 5
	• Generate certification test plan	
Development	• Generate security documentation (operations manual, users manual, security features portion of design specifications)	Chapter 2 Section 3 & Appendix 5
	• Conduct training of security implementation standards and practices	Chapter 8
	• Update system security plan	Chapter 2, Section 3
	• Generate certification test procedures	Chapter 3
	• Identify and mitigate vulnerabilities.	Chapter 2, Section 4
Test and Evaluation	• Identify and mitigate vulnerabilities	Chapter 2, Section 4
	• Conduct certification tests and document results	Chapter 2, Section 5 & Chapter 6
	• Certify application	Chapter 2, Section 6
	• Authorize system	Chapter 2, Section 6
	• Update system security plan with as-built documentation, test results, and authorization to operate	Chapter 2, Section 3

Phase	Activities	References
Operations	• Review and update security plan annually	Chapter 2, Section 3
	• Conduct risk assessments as required and identify and mitigate vulnerabilities	Chapter 2, Section 4
	• Prepare acquisition specifications for contractor security operations, if needed	Chapter 3
	• Reinitiate security life-cycle process for major changes	Chapter 2, Section 3
	• Perform security compliance reviews	Chapter 9
	• Maintain and annually test contingency/disaster recovery plan	Chapter 2, Section 7
	• Conduct security test and evaluation (ST&E) in accordance with this Order	Chapter 10
	• Conduct security training and awareness sessions	Chapter 8
Decommissioning	• Securely decommission systems at end of their life	Chapter 2, Section 4
	• Conduct risk assessments as required and identify and mitigate vulnerabilities	Chapter 2, Section 4 & Chapter 12

SECTION 2: DETERMINING THE REQUIRED LEVEL OF PROTECTION

203. INFORMATION CATEGORIES AND BASELINE SECURITY LEVELS (CS LEVELS).

a. All FAA information falls into one or more information categories. An understanding of these categories is the first step in determining the sensitivity of information and the appropriate protective measures (see Table 2-2).

b. CS2 level is the baseline level for all new FAA information systems, including prototypes. Role-based access control is a requirement that is included in CS3. See appendix 5 for details on the CS2 protection profile.

c. Owners of legacy systems, both NAS and operational support, are required to initiate a security plan, to include conducting a risk assessment to determine threats, vulnerabilities and safeguards and take steps to reduce risk to an acceptable level, and keep the risk to that level or less. ISS certification and authorization will be based on the security plan.

d. Requirements for information systems processing classified national security information are beyond the scope of this Order.

e. All FAA information and every FAA information system falls into one of three security levels. These levels, defined in Table 2-3, are based on the negative impact that an adverse event could have on the agency's mission that would be incurred by loss, corruption, or inaccessibility of that information. Table 2-4 shows the relationship among the information categories shown in Table 2-2 and the security levels (CS levels) in Table 2-3. Detailed security requirements for FAA systems are found in the ISO 15408-1: 1999 (E), *Information technology – Security techniques – Evaluation criteria for IT Security*, *Parts I-III*.

Table 2-2. FAA Information Categories

Category		Explanation and Examples
Number	**Name**	
1	Information about persons	Information related to personnel, medical, and similar data. Includes all information covered by the Privacy Act of 1974 (e.g., salary data, social security information, passwords, user identifiers (IDs), EEO, personnel profile (including home address and phone number), medical history, employment history (general and security clearance information), and arrest/criminal investigation history).
2	Financial, budgetary, commercial, proprietary and trade secret information	Information related to financial information and applications, commercial information received in confidence, or trade secrets (i.e., proprietary, contract bidding information, sensitive information about patents, and information protected by the Cooperative Research and Development Agreement). Also included is information about payroll, automated decision making, procurement, inventory, other financially-related systems, and site operating and security expenditures.
3	FAA internal administration	Information related to the internal administration of FAA. Includes personnel rules, bargaining positions, and advance information concerning procurement actions.
4	Investigation, intelligence-related, or sensitive security information (14 CFR PART 191)	Information related to investigations for law enforcement purposes; intelligence-related information that cannot be classified, but is subject to confidentiality and extra security controls. Includes security plans, contingency plans, emergency operations plans, incident reports, reports of investigations, risk or vulnerability assessments certification reports; does not include general plans, policies, or requirements.
5	Other Federal agency information	Information, the protection of which is required by statute, or which has come from another Federal agency and requires release approval by the originating agency.
6	New technology or controlled scientific information	Information related to new technology; scientific information that is prohibited from disclosure to certain foreign governments or that may require an export license from the Department of State and/or the Department of Commerce.
7	Mission-critical information	Information designated as critical to an FAA mission, includes vital statistics information for emergency operations as cited in FAA Order 1900.1.
8	Operational information	Information that requires protection during operations; usually time-critical information.
9	Life-critical information	Information critical to life-support systems (i.e., information where inaccuracy, loss, or alteration could result in loss of life).
10	Other sensitive information	Any information for which there is a management concern about its adequate protection, but which does not logically fall into any of the above categories. Use of this category should be rare. Contact SSE for assistance.
11	System configuration management information	Any information pertaining to the internal operations of a network or computer system, including but not limited to network and device addresses; system and protocol addressing schemes implemented at FAA; network management information protocols, community strings, network information packets, etc.; device and system passwords; device and system configuration information.
12	Public information	Any information that is declared for public consumption by official FAA authorities. This includes information contained in press releases approved by the Office of Public Affairs, Office of Civil Aviation Security or other official FAA source. It also includes Information placed on public access world-wide-web (WWW) servers.

Table 2-3. Security Levels for Information Systems

CS Security Level	Impact Description	Explanation
CS1	Moderately serious	• Noticeable impact on FAA's missions, functions, image, or reputation. A breach of this security level will result in a negative outcome; OR • Will result in DAMAGE, requiring repairs, to an asset or resource.
CS2	Very serious	• Severe impairment to FAA's missions, functions, image, and reputation. The impact will place FAA at a significant disadvantage; OR • Will result in MAJOR damage, requiring extensive repairs to assets or resources.
CS3	Severe or Catastrophic	• Complete loss of mission capability for an extended period; OR • Will result in the loss of MAJOR assets or resources or could pose a threat to human life.

Table 2-4. Relationship Between Information Categories and *Minimum* Security Levels for IS

Information Category		*Minimum* CS Security Level		
#		CS1	CS2	CS3
1	Information about persons		X	
2	Financial, budgetary, commercial, and trade secret information		X	
3	FAA internal administration		X	
4	Investigation, intelligence-related, and security information			X
5	Other Federal agency information		X	
6	New technology or controlled scientific information		X	
7	Mission-critical information			X
8	Operational information		X	
9	Life-critical information			X
10	Other information	X*		
11	System configuration management information		X	
12	Public information	X*		

NOTE: *This information may vary. Contact the ISSD or ISSC for guidance.

c. A security level must be assigned to all FAA information systems. The majority of FAA information falls into security levels CS2 and CS3. The information owner must analyze the sensitivity, criticality, impact, the harm of potential loss and risk assessment in order to accurately determine the correct security level. As a result of this analysis, the minimum security level may be increased or decreased from what is outlined in Table 2-4. Understating security level may result in vulnerabilities to the FAA infrastructure. Overstating security level could result in having increased requirements and costs

levied on an information system. The information owner is encouraged to consult the ISSD or ISSC for assistance in determining the appropriate security level. The security level should be reevaluated at least every 3 years by the system owner because influencing factors may change.

d. The security level of an IS must be at least as high as the level of the most sensitive information that is being processed, or will be processed, by that application. NOTE: COTS applications used to process sensitive data will be rated based on the sensitivity of the data processed.

e. The ISS plan shall indicate how the system's security level was determined.

SECTION 3. INFORMATION SYSTEM SECURITY PLAN

204. PURPOSE. An ISS plan provides an overview of ISS requirements and describes how and when those requirements are being met or will be met. An ISS plan may also be viewed as documenting the process of planning adequate, cost-effective security protection for an information system.

205. REQUIREMENTS. Every FAA information system must have an ISS plan to be consistent with the Computer Security Act of 1987 and OMB Circular A-130, Management of Federal Information Resources, Appendix III.

206. SCOPE. ISS plans are determined as follows for the various applications used at the FAA:

a. A general support system must be covered by an ISS plan, as the system is an interconnected set of information systems with the same direct management control and with a common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, operational rules and procedures, and people. It provides support for a variety of users and applications. Examples of general support systems include local area networks (LANs), Virtual Private Networks (VPNs), Regional Backbones, Metropolitan Area Networks (MANs) communications networks such as the Leased Interfacility National Airspace System Communication System (LINCS), the Agency Data Telecommunications Network 2000 (ADTN-2000), and the Alaska Interfacility Communications System (ANICS).

b. A major application or system must be covered by a separate ISS plan. As defined in OMB Circular A-130, Appendix III, a major application is an application "that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of" its information. A major application may be comprised of many hardware, software, and telecommunications components. These components may include software applications or combinations of hardware and software that support a specific mission-related function; they may also include facilities, procedures, and operators. Examples of such major FAA applications include the Wide Area Augmentation System (WAAS), the Network Information Management System (NIMS), and the Integrated Payroll and Personnel System (IPPS). A major application may also consist of several applications that are all related to a single mission function; an example of this type of major application is the Civil Aviation Security Information System (CASIS). A major application may be geographically distributed, while still being covered by a single ISS plan. A major application may include other major applications, each having its own ISS plan.

c. FAA applications may be covered by the ISS plans for the general support system on which they run or for the major application of which they are a part. For example, a regional or facility program designed to track expenditures against a budget might be covered by a general support system security plan for an office automation system or for a LAN. Similarly, standard commercial off-the-shelf (COTS) general purpose software, such as word processing or e-mail software, would typically be covered by the plans for the general support system on which it is installed. Major application ISS plans must address any general support systems that may process, transmit, or store the major application's data. See par 234 for interconnection requirements.

207. RELATIONSHIP TO THE SYSTEM LIFE CYCLE.

a. The ISS plan must be part of the input to the Acquisition Review (AR) for system funding decisions. It must also be part of the input to the acquisition process, development, and operation of every

new FAA information system. Similarly, as each existing system is subjected to the security certification and authorization process, the ISS plan will become part of its operation, maintenance, and enhancement requirements.

b. The ISS plan must be developed early in the acquisition phase of every new contract-developed FAA information system and developed during the initiation phase of FAA-developed systems, and maintained throughout the system's life cycle (see Table 2-1). A preliminary ISS plan should be generated as part of the mission needs analysis process. As the system nears the development phase, the ISS plan's emphasis should shift to cover the ways that the system will be protected in the development environment and the ways that will ensure compliance with applicable security requirements. Another shift should occur in preparation for the system's going operational when increased emphasis should be placed on the operational safeguards to be used. Further revisions should take place, to the extent needed, each time the system is to be recertified and reauthorized. The final shift will occur when the system enters the decommissioning phase.

c. Locally purchased or developed systems do not negate inclusion of security in the life cycle. Purchases and development must be in accordance with the Acquisition Management System (AMS), of which the security life cycle is a part. Purchase or development of a product without consideration of security from the initiation phase of the life cycle through decommissioning could have an adverse effect on other systems interfaced with an unprotected system.

208. RESPONSIBILITIES.

a. The project or product team's lead is responsible for a system's design, development, and enhancement. The lead must ensure that an ISS plan is prepared, implemented, and maintained and that its effectiveness is monitored, during those activities. Similarly, the program manager responsible for a fielded system must ensure that an ISS plan is prepared (if it does not already exist), implemented, and maintained, and that its effectiveness is monitored during the system's operational life. The DAA is the approving authority for the ISS plan.

b. The ISS Division will advise the Joint Resources Council (JRC), or the project team for FAA-developed systems, on the acceptability of each ISS plan at each significant stage of the covered system's life cycle.

c. The ISS plan must be included in the material presented at the AR for contract-developed systems and must be formally approved at that time. FAA-developed systems' ISS plans must be formally approved prior to fielding. A copy of the approved ISS plan must be provided to the ISS Division manager and to the DAA following the AR.

d. Project teams or program offices for locally purchased or developed systems will follow paragraph 210(a) of this section and will coordinate and submit the security plan for review to the ISSC within region/center SSE.

e. Small purchases of software or use of privately owned software must be coordinated with and approved by the system owner, who is responsible for confidentiality, integrity and availability of information, before purchase or installation. Failure to coordinate prior to installation may result in an adverse effect on the availability of information to other users. The system owner has the authority to remove any software that does not have prior written approval for installation.

209. THE SECURITY PLAN PACKAGE: CONTENT AND FORMAT.

a. Each FAA ISS plan package must include a detailed description of the system and its components, an identification of the system's sensitivity, identification of the applicable protection requirements, and a list of the security measures or controls that are currently being used or will be used to protect the system's components. Documents that must be included are the risk assessment, security test and evaluation (ST&E), certification and authorization. The type of system and information may require inclusion of other documents such as a site survey. Appendix 4 provides an outline for an ISS plan.

b. All ISS plans must be prepared according to the appropriate (major application or general support system) format outlined in Appendix 4. Further guidance is provided in NIST's *"Guide for Developing Security Plans for Information Technology Systems"*.

c. The level of detail in the ISS plan must be based on the requirements appropriate to the system's security level. The ISS plan must fully identify and describe the controls currently in place or planned for the system. The control measures covered must include development and implementation controls, administrative and operational controls, security awareness and training, physical security measures, and technical controls.

d. The level of detail in various parts of the ISS plan must also be consistent with the system life-cycle phase.

210. ISS PLAN PACKAGE SENSITIVITY, HANDLING AND MAINTENANCE.

a. Each ISS plan package must be marked, handled, and controlled in accordance with Chapter 7 of this Order.

b. All ISS plans must be dated or numbered for ease of tracking modifications and approvals.

c. As part of configuration management (CM) (see Chapter 4 of this Order), all approved ISS plan versions, plus the most recent version of any draft ISS plan later than the latest approved plan, must be included in the security library (see par 401). Each approved version of an ISS plan package must have its' certification, authorization and other background documents.

d. A copy of the final ISS plan package will be forwarded to the ISS Division or the regional/center SSE as appropriate.

e. ISS reauthorization will be conducted as specified in par 244.

f. The security plan package will be maintained for the system life cycle plus one year after decommissioning by the program or system owner and the ISS Division or the SSE.

211 - 219. RESERVED.

SECTION 4. INFORMATION SYSTEM SECURITY RISK MANAGEMENT

220. SYSTEM SECURITY PLAN. Risk management is a crucial element of the system security planning process. The data gathered during an ISS risk assessment supports management in decisions about the most appropriate security measures for an information system. The risk assessment for each information system will be included in the security plan package.

221. ISS RISK MANAGEMENT.

a. Risk is the possibility of an adverse event that causes loss or damage. Risk has many different components: assets, threats, vulnerabilities, safeguards, and consequences. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and keeping risk to that level or less. ISS risk management addresses risks that arise from an organization's use of information technology. There are several considerations for computer-based risk:

(1) The type of risk may be different from risks previously associated with the organization or function.

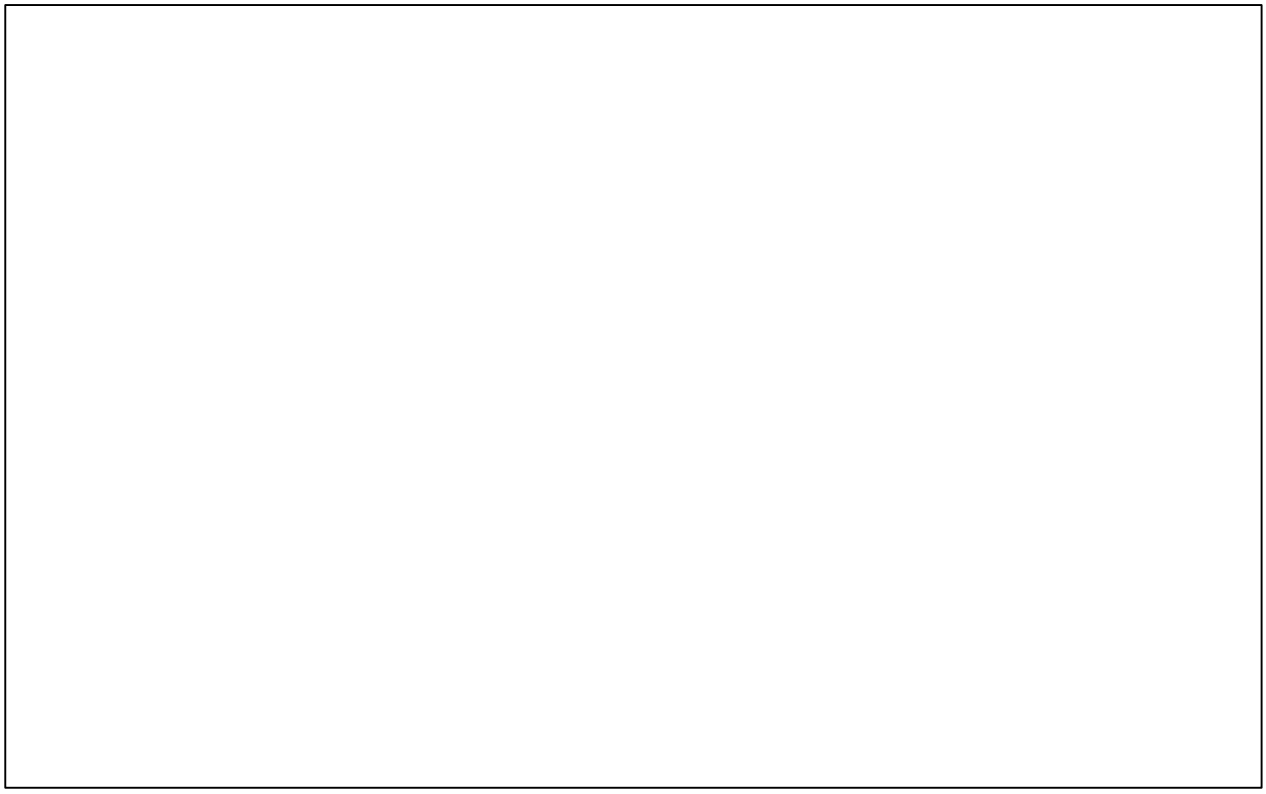
(2) The proliferation and decentralization of computing power can make it difficult to identify key assets that may be at risk.

b. Facilities security risk management is addressed in FAA Order 1600.6, FAA Physical Security Management Program. FAA Order 1600.6 addresses risk that is based on environment and on the physical boundaries of and within the FAA facility.

222. RISK ASSESSMENT. OMB Circular A-130**,** Appendix III, specifies an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. Commercial

risk assessment products are available and may be used. Risk assessment is comprised of three basic activities: determining the assessment's scope, collecting and analyzing data, and interpreting risk assessment results.

Table 2-5. Risk Assessment Process



a. Determining the Assessment's Scope. The first step in assessing risk is to identify the system under consideration, the part of the system that will be analyzed, and the analytical method for determining risk, including the level of detail and formality. Determining the boundary of a system is crucial. An information system's boundary determines the system interfaces and what is inside and outside of the boundary parameters. The methodology chosen provides a consistent format by which to assess risk.

b. Collecting and Analyzing Data. The second step involves collecting and analyzing the information to determine interrelationships and impacts and to evaluate plans for mitigating potential, residual risks. This step includes the following elements:

(1) Screening of information. To avoid unnecessary expense, screening techniques should be used to limit the overall effort and the amount of information gathered. Data threats and vulnerabilities should be ranked, and the risk management effort should focus on those areas that could result in the greatest harm to the organization.

(2) Asset valuation. If the quantitative risk analysis methodology is chosen for all or part of a risk assessment, then assets, including information, software, personnel, hardware, and physical assets (such as a computer facility), must be identified. The value of an asset includes its intrinsic value and the near-term impacts and long-term consequences of its compromise. FAA Order 1600.6 provides further information on collecting data about assets within the FAA.

(3) Consequence assessment. The consequence assessment estimates the degree of harm or loss that could occur. Consequence refers to the overall, aggregate loss that occurs. While exploitation of an asset often results in disclosure, modification, destruction, or denial of service, consequences result in more significant, long-term effects, such as failure to perform the system's mission, loss of integrity, violation of privacy, injury, or loss of life. The more severe the consequences of an asset being exploited, the greater the risk to the system and to the organization.

(4) Threat identification. A threat is an entity or event with the potential to harm the system. Threats should be identified and analyzed to determine the likelihood of their occurrence and their potential to harm information systems. Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses—from unintentional harm to a database's integrity to fires that destroy entire computer centers. The risk analysis should concentrate on those threats most likely to occur and affect important assets. Some threats may combine elements from more than one area of the following common threats: employee sabotage, loss of physical and infrastructure support, malicious hackers, industrial espionage, introduction of malicious code, foreign government espionage, terrorism, organized crime, natural disasters, and threats to personal privacy.

(5) Threat stipulation. "*The FAA Information Security Threat Stipulation*" report, prepared and administered by the Office of Civil Aviation Security Intelligence (ACI) and the ISS Division, stipulates the anticipated types of threats to FAA systems and the types of security attacks that these systems are expected to withstand. Because FAA systems face similar threats, this document will allow FAA organizations to plan for, and mitigate, a consistent level of threat across systems. The ISSM may obtain a copy of this report from the ISS Division. Regional/center ISSOs may contact the ISSC to obtain copies of threat information.

(6) Vulnerability analysis. A vulnerability is an absence or weakness in security procedures, technical controls, physical controls, or other controls that could be exploited by a threat. Vulnerabilities are often analyzed in terms of the insufficiency of implemented safeguards.

(7) Methodology.

(a) Risk analyses shall be used to evaluate the security posture of an existing system. The results are typically represented as qualitative and quantitative.

(b) Qualitative analyses are descriptive and express threats, likelihood of exploitation, and loss in such terms as high, medium, or low, or in rankings on a scale of 1 to 10.

(c) Quantitative analyses express threats and likelihood of exploitation as percentages and expresses the loss in terms of dollars, as annualized loss expectancies or single occurrences of loss. The quantitative approach is used for the physical environment, which is addressed in FAA Order 1600.6.

(d) Appendix 4 contains a sample ISS risk assessment outline. It may be used by any organization as an example. A copy of the risk analysis must be included in the security plan package.

c. Interpreting risk assessment results. The third step is interpreting the results of the risk assessment. The interrelationship of vulnerabilities, threats, and assets (data or system) is critical to analyzing risk. Threats may exploit vulnerabilities in the system and cause harm to the data or to an entire information system. To protect the assets, safeguards must be implemented to eliminate or mitigate vulnerabilities. The risk assessment process shall support two related functions: accepting risk and selecting cost-effective controls. To accomplish these functions, the risk assessment must produce a meaningful output that reflects what is truly important to the organization and its mission.

223. SAFETY RISK MANAGEMENT.

FAA Order 8040.4, Safety Risk Management, states that a formal, disciplined, and documented decision-making process shall be used to address safety risks in relation to high-consequence decisions impacting the complete product life cycle. The critical information resulting from a safety risk management process can thereby be effectively communicated in an objective and unbiased manner to decision-makers, and

from decision-makers to the public. All decision-making authorities within the FAA shall maintain safety risk management expertise appropriate to their operations, and shall perform and document the safety risk management process prior to issuing the high-consequence decision. Safety and security risk assessment have some common or overlapping areas, of which three are discussed below.

a. Data collection. The data collected for an information system is used for both types of assessment with some variations.

b. Vulnerability analyses and risk mitigation. As discussed in paragraphs 222 and 224 of this Order, vulnerabilities will be identified and safeguards will be recommended to mitigate risk. This is where safety and security overlap. The vulnerabilities identified in one process will not change for the other process. The melding of the data for the two assessment types at this point will identify safety and security concerns that may impact decision-making

c. Risk acceptance. Security certification of a system requires that the risk assessment include the residual risk after mitigators are applied before final authorization, which is the acceptance of risk. Including the hazard identification, as well as other safety data in the security risk assessment process will result in the availability of more accurate information for the decision-makers.

224. RISK MITIGATION. Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management, within applicable constraints. The process of risk mitigation has flexibility, and the sequence will differ, depending on data sensitivity, physical controls, environment, available funding, and other factors.

a. Safeguards (Countermeasures). A safeguard is any action, device, procedure, technique, or other measure that reduces the likelihood of a threat to a system. Safeguard analysis should include an examination of the effectiveness of the existing or proposed security measures. This analysis shall identify new safeguards that could be implemented in the system.

b. Considerations. A primary function of information security risk management is the identification of appropriate controls. In designing or reviewing a system's security, it may be obvious that some controls should be added (e.g., because they are required by law or are clearly cost effective) and that other controls may be prohibitive in terms of monetary and non-monetary factors. However, in selecting appropriate controls, managers need to consider many factors, including organizational policy, legislation, and regulation; safety, reliability, and quality requirements; system performance requirements; timeliness, accuracy, and completeness requirements; life-cycle costs of security measures; and technological feasibility.

c. Safeguard Alternatives. When being selected, safeguard alternatives must be analyzed to determine that the sets of alternatives can work together to protect the system from known threats. Often, a safeguard must be used in concert with other safeguards (for example, audit tracking software must be monitored and the output analyzed in order to determine if the software is effective). Security measures that are chosen only to meet a requirement and are not linked with other safeguards result in inefficiencies and vulnerabilities that may increase costs and affect the information system's availability, integrity, and confidentiality.

d. Selection Methods. Two methods are available to assist management in the safeguard selection process: situational (what if) analysis or system security measures. One of these methods must be completed and the documentation included as part of the risk assessment.

(**1) Situational analysis (what if).** This analysis looks at the costs and benefits of various combinations of controls to determine the optimal combination for a particular circumstance. The effect of adding various safeguards is tested to see what difference each makes in terms of cost, effectiveness, and other relevant factors. The analysis of tradeoffs supports the acceptance of residual risk. This method typically involves multiple iterations to see how proposed changes will affect the result. Computer security personnel use the results of this analysis to make a recommendation to their management officer, who then weighs the costs and benefits, takes into account other constraints (e.g., budget), and selects a solution. For more information about what-if analysis, see NIST S.P. 800-12, An Introduction to Computer Security: The NIST Handbook, Chapter 7.

(2) System security measures. This method categorizes types of safeguards and recommends their implementation based on the information system's level of risk. For example, stronger controls would be implemented on high-risk systems than on low-risk systems. For more information about this method, see DOT H 1350.251, Appendix F, part III, which contains preconfigured security controls used for baseline controls.

225. RISK ACCEPTANCE. Like the selection of safeguards, risk acceptance should consider various factors other than those addressed in the risk assessment. Risk acceptance is linked to the selection of safeguards: the safeguards may be too expensive (in either monetary or non-monetary terms) or may exceed current technical capabilities.

226. AUTHORIZATION OF A SYSTEM. Residual risk is the risk that remains after safeguards are implemented. The DAA must decide if the operation of the computer system is acceptable, given the type and severity of remaining risks. Within the FAA, the acceptance of risk is closely linked with the authorization to use an information system. Authorization is the written acceptance of risk by the DAA to permit a major application or general support system to process sensitive information in an operational environment in performance of the FAA mission. (See Chapter 2, Section 7).

227. LIFE CYCLE AND RISK ASSESSMENT. Security risk is associated with every part of the life cycle of an information system. Therefore, ensuring that security risks do not reach an unacceptable level is a process that must extend from the conceptual stage of a specified information system throughout its life cycle and eventual disposal or exit from the FAA's responsibility. See Table 2-6 for an overview of the life cycle risk assessment activities.

Table 2-6. Risk Assessment Activities in Life Cycle Phases.

a. Initiation. During this phase of the life cycle, the ISS plan is initiated. An ISS risk assessment is conducted, based on initial requirements, to discover security vulnerabilities that may exist. Safeguards are implemented, leading to an updated initial requirements document.

b. Definition. Once the initial ISS risk assessment is completed, subsequent risk assessments are conducted based on a system's progression through the acquisition and software completion processes. Focusing on the major vulnerabilities discovered through risk assessment will save resources. Documentation is attached to the initial ISS risk assessment and becomes a permanent part of the security plan package, resulting in a baseline for risk assessments conducted during the remainder of the life cycle.

c. Design. After the ISS risk assessment is completed and appropriate safeguards are selected, those safeguards need to be effectively implemented. Subsequent ISS risk assessments will be conducted during all testing phases and in anticipation of major system or physical environment changes.

d. Development. Technical safeguards are not always feasible because of expense or interference with the system's reliability. Personnel and physical security measures will be taken to augment technical safeguards and will be documented in ISS risk assessments. An ISS risk assessment shall be conducted at least once every 3 years as part of the recertification process or when a major change to the system's operational or threat environment occurs. The ISS risk management process provides a history of security activity throughout an information system's FAA life.

e. Test and Evaluation. All test results and evaluations will be included as part of the security plan package. Any vulnerabilities discovered during testing will be recorded in the ISS risk assessment.

f. Operations. ISS risk assessments will be conducted in anticipation of major system or physical environment changes, such as decommissioning. Risk assessments will also be conducted when new vulnerabilities or threats are discovered which affect the system. ISS risk assessments will be added to the security library and to the initial plan and will remain with the security plan package.

g. Decommissioning of systems. Decommissioning of systems is a major system change and requires a risk assessment. See Chapter 12 for further information.

228 - 229. RESERVED.

SECTION 5. ISS CERTIFICATION

230. GENERAL PROVISIONS.

a. Certification is a statement based on the comprehensive testing and evaluation of the technical ad non-technical security features of an information system, and other safeguards, made in support of the authorization process. It establishes the extent to which a particular information system design, implementation, and operation meet the security requirements documented in the ISS plan. Certification primarily addresses software and hardware security safeguards, but also considers procedural, physical, personnel, and other security measures used to enforce ISS policy and reduce risk.

b. Certification is a requirement for all FAA information systems, NAS, NAS-support and administrative, including legacy and prototype systems, and is conducted at the time and in the sequence specified in the ISS plan

c. The Certifying Team (CT) is responsible for developing the security plan, conducting the risk assessment, and coordinating security testing efforts. Based on these efforts, the CT assesses system compliance with stated security requirements. The CT documents and presents identified risks and mitigating factors to the CO with a request for certification and a recommendation on authorization. The CT coordinates with their ISS Division point of contact (POC) during the development of all security documentation. The ISS Division POC will coordinate all certification and authorization efforts with the CT and the CO as a representative of the Certifying Agent.

d. The Certifying Agent (CA) is responsible for determining if the system is in compliance with stated requirements for certification and authorization. The CA reviews all documentation presented in support of the certification and authorization process, assesses the risks associated with operating the system, and makes recommendations to the CT, CO, and the Designated Approving Authority. In addition, the CA coordinates the certification and authorization activities and consolidates the final certification and authorization packages for submittal to the DAA (NOTE: this responsibility is delegated to the ISS Division POC for a given system). The CA is the ISS Division Manager.

e. The Certifying Official (CO) is a senior management official responsible for making a technical judgement of the information system's compliance with stated security requirements. The CO formally requests approval to operate from the DAA. The CO presents all security documentation, including the recommendations of the CT and CA to the DAA for review and acceptance. The Certifying Official is from the line of business responsible for the development of the system.

f. The ISS Division Manager may designate, in writing, a region or center Certifying Authority (CA). This Certifying Authority (CA) shall oversee or conduct ISS certification for locally developed information system(s) as indicated in the appointment letter. The letter may be for a single system or multiple systems.

g. The DAA is the official with the authority to accept or not accept the security safeguards prescribed for a system and formally assume responsibility for operating a system at an acceptable level of risk. The DAA is an Associate Administrator from the organization that will implement, own, operate, and maintain the system.

h. The certification portion of the ISS package shall contain all security documentation, including, the system security plan, risk assessment, security test procedures and results, and managerial memos necessary for certification. This package shall be maintained under CM control throughout the system life cycle. This procedure permits reuse of the appropriate documentation during re-certification.

231. CERTIFICATION PROCESS.

a. Prior to its authorization, each information system shall be evaluated and tested to ensure that it meets all applicable Federal and FAA policies, regulations, and standards, as documented in its ISS plan (Chapter 2, section 4), and that all installed security safeguards appear to be functional, adequate, effective, and appropriate for the protection requirements of the information system. Certification

culminates in a Security Evaluation Report that provides and executive summary of risks, mitigation, and recommended corrective action, and a Security Certification Statement that indicates system compliance to stated security requirements, and provides recommendations for authorization. The Security Certification Statement is signed by the Certification Team, Certification Agent, and the Certification Official. The Security Evaluation Report and signed Security Certification Statement are forwarded to the DAA with a formal request for authorization. The ISS Division point of contact will assist in development and signature coordination of this documentation. A sample Security Evaluation Report is provided in appendix D.

b. Prior to certification or recertification, an independent, onsite, ISS inspection and verification review may be conducted to verify that adequate and appropriate levels of protection are being provided for the individual systems, based on their unique protection requirements. The ISS evaluation team will be under the direction of the ISS Division manager or designee (Chapter 9).

232. TYPE CERTIFICATION. When an information system is installed in multiple locations, it may be more expedient and efficient to perform a type certification that addresses all the common characteristics. An additional site-specific certification is then performed for each instance of the information system. Certification testing of system interconnections would occur primarily during site-specific certification tests. The decision to permit type certification rests with the CA.

233. SOFTWARE CERTIFICATION. This certification includes inspection of the system's configuration management (CM) documentation to ensure that the composition of the system being certified is known in all details and can be identically re-created, that the master copy of the software is adequately protected and backed up, that documentation has been controlled, and that all commercial software has been acquired in a secure manner. Various software will be certified in the following ways:

a. FAA-Developed Software. For this software, design reviews and system tests shall be performed, and a certification of the results shall be recorded for existing software when significant modifications are made and for newly developed software to ensure that there are no features that are detrimental to FAA IS security.

b. GOTS. This software shall be examined to ensure that the software does not contain features that might be detrimental to FAA IS security. Software design reviews, documentation reviews, and systems tests will be performed, and a certification will be recorded when significant modifications are made to GOTS software.

c. COTS. This software shall be examined to ensure that the software does not contain features that might be detrimental to FAA IS security. Security-related software and documentation shall be examined to ensure that the security features function as specified.

234. INTERCONNECTION.

a. The interconnection of two information systems requires certification and authorization. The certification documentation shall include a formal interconnection agreement between the DAAs (see par 240) to record interface restrictions, limitations, and constraints associated with the interface devices used for connection and any other restrictions. The DAA of each system shall maintain copies of the other system's interconnection agreement, certification, and authorization reports as part of the security plan package. Telecommunications systems must only list systems connected to it as part of the risk assessment, unless a system proves to be a vulnerability to the telecommunications system. However, IS connected to telecommunications systems must seek an interconnection agreement.

b. The interconnection agreement shall address applicable, security-related policies and identify any restrictions or new security services and assurances that must be added. It must also document any procedures or operational constraints placed on the system by virtue of the interconnection.

c. Managerial issues to be addressed in the interconnection agreement shall include a general description of information transmitted through the interconnection, a summary discussion of trusted behavior expected from each IS, description of overall security policy, description of additional security training and assignment of training responsibility, and description of the user community.

d. Technical issues to be addressed in the interconnection agreement shall include:

(1) Specification of the security parameters to be transmitted between communicating information systems.

(2) Security details relevant to the exchange of information among information systems (e.g., data tags).

(3) Any special considerations for dial-up connections (e.g., authentication).

(4) Description of security protections provided by data communications, both local to a system and between communicating systems.

(5) Description of the information that each information system will log in an audit trail and the way audit trail tasks will be divided and shared among information systems.

(6) Description of the information security services provided by each information system.

e. Interconnection with the Internet shall include extraordinary protection, for example, system isolation devices (screening routers, firewalls). The information system shall have a prepared contingency plan that addresses responses to penetrations, viruses, denial-of-service attacks, and other similar threats that are inherent to an Internet connection.

235. TRANSITION AND PHASE-IN. Each organization directly reporting to AOA-1 shall develop an overall plan for the certification and authorization of all FAA information systems under the manager's jurisdiction and in use when this Order is issued. A schedule for information system-wide certification and authorization shall be issued and a copy of the schedule shall be forwarded to the ISS Division each fiscal year. This schedule will be updated annually.

236 - 239. RESERVED.

SECTION 6. AUTHORIZATION

240. GENERAL PROVISIONS. An authorization is a written declaration by the DAA that a system is approved to operate in a particular environment using a prescribed set of safeguards. The approval to operate is based on the certification process, including the recommendations of the Certifying Official and Certifying Agent, as well as other management considerations. The Authorization Statement affixes security responsibility with the DAA and demonstrates that due care has been taken identifying, assessing, and documenting the risks to the system. Authorization is required for all general support systems, major applications, and system interconnections. No new FAA information system shall be permitted to operate until that operation has been authorized.

241. DESIGNATED APPROVING AUTHORITY.

a. The DAA shall issue a statement that records the decision to authorize a system to process information in the performance of the FAA mission. The authorization statement affixes security responsibility with the DAA and shows that due care has been taken for security. The ISS Division POC will assist in developing the authorization statement.

b. The minimum documentation for information system certification and authorization shall consist of the ISS plan; Risk Assessment; security test results; Security Evaluation Report; Certification Statement; formal authorization request letter; and security documentation for system administrators and users. (See Chapter 2, Section 3).

c. Prior to activation, the interconnection between an FAA information system and any other information system must be authorized by the DAA, based on the acceptance of risk to the system. Connection shall be contingent on the presence of the controls that are consistent with the rules of the systems. (See Chapter 2, Section 6).

d. OPS support systems connecting with NAS operational systems must obtain the signature of the ATS DAA for an interim authorization as well as the DAA of the operational support system.

e. The DAA shall weigh the recommendations of the Certifying Official and Certifying Agent. The DAA shall confirm that the authorization evidence is sufficient, adequate, and accurate to justify authorizing system operation and accept associated risks. If the DAA is not satisfied with the documented or planned safeguards, a denial of authorization may be issued.

f. The DAA shall ensure that each authorized system is reviewed at least every 3 years or whenever a significant change occurs in the information system or the environment.

242. INITIAL AUTHORIZATION.

a. The DAA shall review the certification documentation and shall decide whether the information system is granted a final approval to operate (authorization), is given an interim approval to operate (interim authorization) for a specific period of time pending satisfactory completion of specified tasks, or is denied approval to operate (denial of authorization) until identified deficiencies are corrected.

b. If the information system is approved to operate, the DAA shall sign a formal authorization statement declaring that the system appears capable of operating at an acceptable level of risk. The statement may also define any conditions or constraints required for appropriate system protection, including corrective action.

243. INTERIM AUTHORIZATION.

a. Interim authorization to operate may be granted for a fixed period of time, not to exceed 1 year. This authorization is based on acceptable, although perhaps incomplete, authorization documentation and is contingent on certain conditions being met. The interim authority to operate, while continuing the authorization process, permits the information system to meet its operational mission requirements while improving its security posture. A recommendation or request for an interim authorization may be made by CO. Interim authority to operate is not a waiver of the requirement for authorization. The information system must meet all requirements and receive final authorization to operate by the expiration date of the interim authorization.

b. An extension of an interim authorization may be granted only by the DAA with concurrence from the ISS Division Manager.

c. Prototype systems shall not be connected until final or interim authorization is received as specified in paragraph 250.

d. Authorization statements for operational support systems connecting with NAS operational systems must obtain the signature of the DAA for the operational support systems, as well as the signature of the DAA for the operational NAS system.

244. REAUTHORIZATION.

a. Systems shall be recertified and reauthorized when major changes occur to the system or every 3 years, whichever occurs first. Major changes include, but are not limited to, the following conditions or events:

(1) A significant change occurs in the hardware, software, or data communications configuration that impacts the ISS safeguards defined in the original authorization package.

(2) The sensitivity level of the information being processed is significantly changed.

(3) The threat environment changes.

(4) The information system facility undergoes changes, for example, a major office relocation, structural modifications, or other significant changes that may affect ISS.

(5) A security-related event occurs that appears to invalidate the existing authorization.

b. The revision and review process certification and authorization shall include the same steps required for the original certification and authorization. Parts of the original documentation need not be redone, but documentation must be updated to address any security-relevant changes to the system and/or environment. The ISS Division point of contact will provide guidance for recertification and reauthorization.

c. If a system is undergoing significant modification when its authorization to operate expires, the DAA may issue an interim authorization of the existing system to facilitate completion of modifications. This type of interim authorization may be renewed by the DAA as long as the system is actively undergoing significant modifications. This paragraph does not apply to prototypes, only to existing or legacy systems.

245 - 249. RESERVED.

SECTION 7. CONTINGENCY PLANNING

250. GENERAL. OMB Circular A-130 specifies contingency plans for every information system. An information system contingency is an event with the potential to adversely affect information system operations and thereby disrupt critical mission and business functions. Such events include power outages, hardware failures, malicious attacks, fires, or storms. If an event is very destructive, it is often called a disaster. To avert these potential contingencies and disasters or minimize their damage, organizations must take steps early to control such an event. This contingency planning directly supports an organization's goal of continued operations. Contingency planning is closely related to incident handling, which primarily addresses malicious technical threats such as hackers and viruses. Contingency plans for information systems must be developed in conjunction with facility security and contingency plans mandated by FAA Order 1600.6, Physical Security Management Program and, if applicable, FAA Order 1900.47, Air Traffic Services Contingency Plan.

251. REQUIREMENTS. The requirements for contingency plan development, test, maintenance and disaster recovery are applicable to all general support and major application information systems that support FAA operational or administrative missions where unplanned service disruption would critically affect the mission.

a. New Plans. The system owner shall be responsible to ensure that the contingency plan is completed and updated. The contingency plan should formally designate personnel, by position, to carry out the plan. These individuals shall be informed of their responsibilities and shall participate in tests of the plan. Reference to the appropriate contingency plan must be included in the ISSP. However, system specific contingencies must be included in the ISSP Package as part of the certification process.

b. Existing Plans. In accordance with FAA Order 1600.6 and FAA Order 1900.47, facility managers are responsible for contingency plans related to their facilities. If a contingency plan has been completed under another FAA Order, such as FAA Order 1600.6 or, if applicable, FAA Order 1900.47, then any ISS contingencies that were not included in the existing plans must be incorporated. Reference to the appropriate contingency plan must be included in the ISSP.

252. OBJECTIVE. The objective of the plan is to provide reasonable continuity of information system support, should events occur that prevent normal operations. The plan must be fully documented and operationally tested periodically, at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption or denial of service.

253. PROTECTION OF CONTINGENCY PLANS. According to 14 CFR 191.7, contingency plans are listed as sensitive security information and will be marked and protected in accordance with Appendix 8.

254. CONTINGENCY PLAN DEVELOPMENT. Contingency planning involves more than planning for a move offsite if a disaster destroys a data center. It also addresses how to keep an organization's critical functions operating in case of disruptions, both large and small. The contingency planning process is covered in six steps:

a. Step 1. Identify Mission- or Business-Critical Functions. The definition of an organization's critical mission or business function is called a business plan. Because the development of the business plan will be used to support contingency planning, it is necessary, not only to identify critical missions and business processes, but also to set priorities and time criticalities for them. The system owner is responsible for ensuring completion of the business plan and for prioritizing the recovery needs for the organization's critical functions. Because a fully redundant capability for each function is prohibitively expensive for most organizations, certain functions will not be performed in case of a disaster. If appropriate priorities have not been set, it could make a difference in the organization's ability to survive a disaster.

b. Step 2. Identify Resources That Support Critical Functions. After critical missions and business functions are identified, supporting resources should be identified, as well as the timeframes in which each resource is used, and the effect of unavailable resources on the missions. Contingency planning should address all the resources needed to perform a function, including personnel, processing capability, system applications, computer-based services, physical infrastructure, and documents and papers.

c. Step 3. Anticipate Potential Contingencies or Disasters. Although it is impossible to anticipate everything that can go wrong, this step involves identifying a likely range of problems. Developing scenarios can help an organization prepare a plan to address the wide range of possible mishaps. Scenarios should include small and large contingencies that require both short-term and long-term responses. Incident response planning should be included in this step, as discussed in Chapter 10.

d. Step 4. Select Contingency Planning Strategies. This step considers plans to recover needed resources. When alternative strategies are evaluated, current controls for preventing and minimizing contingencies should be considered. Because no one set of controls can prevent all contingencies in a cost-effective manner, prevention and recovery efforts should be coordinated. Risk assessment can also help determine an optimal strategy. A contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption. Emergency response encompasses the initial actions taken to protect lives and limit damage. Recovery refers to the steps taken to continue support for critical functions. Resumption is the return to normal operations. The longer it takes to resume normal operations, the longer the organization will have to operate in the recovery mode. The selection of a strategy needs to be based on practical considerations, including feasibility and cost. Different categories of resources should be considered:

(1) Processing capabilities. For less serious contingencies, processing capabilities can be restored from backups or original media or by repairing equipment components. For a serious contingency, however, the strategies for ensuring processing capability are normally grouped into five categories:

(a) Hot site. A building already equipped with processing capability and other services.

(b) Cold site. A building for housing processors that can be easily adapted for use.

(c) Redundant site. A site equipped and configured exactly like the primary site.

(d) Reciprocal agreement. An agreement that allows two organizations to back up each other.

(e) Hybrids. Any combinations of the above, such as having a hot site as a backup in case a redundant or reciprocal agreement site is damaged by a separate contingency.

(2) Automated applications and data. It is required that the primary contingency strategy for applications and data is regular backup and secure offsite storage. Important issues to be addressed include the frequency of backups, the frequency of offsite storage, and the manner of transporting backups.

(3) Computer-based services. Service providers may offer contingency services. Voice communications carriers often can reroute calls to a new location, and data communications carriers can

also reroute traffic. If one service is down, it may be possible to use another. Resuming normal operations may require such rerouting of communications.

(4) Physical infrastructure. Arrangements must be made for processing capability support, office space, furniture, and more. If the contingency plan calls for moving offsite, procedures need to be developed to ensure a smooth transition back to the primary operating facility or to a new permanent location.

(5) Documents and Papers. The primary contingency strategy is usually backup onto magnetic, optical, microfiche, or other medium and offsite storage. A supply of forms and other needed papers can be stored offsite.

e. Step 5. Implementing Contingency Strategies.

(1) Preparations. To implement strategies for protecting critical functions and their supporting resources, much preparation is needed, including such common preparation as procedures to back up files and applications, to establish contracts and agreements, and to purchase redundant equipment. Preparations, including documentation, must be kept up to date. For small or less complex systems, the contingency plan may be a part of the ISS plan. For larger or more complex systems, the ISS plan could contain a brief synopsis of the contingency plan which would be a separate document.

(2) Responsibility. The system owner has the responsibility to ensure that a written contingency plan is completed. If a contingency plan has been completed under another FAA Order, such as FAA Order 1600.6 or, if applicable, FAA Order 1900.47, then incorporate any ISS contingencies that are not included. Because a written plan is critical during a contingency event, the plan should clearly state in simple language the tasks to be performed in a contingency so that someone with minimal knowledge could immediately begin to execute the plan. All personnel should be trained in their contingency-related duties.

(3) Approval. The completed contingency plan must be approved by the local ISSC.

(4) Availability. It is helpful if up-to-date copies of the contingency plan are available in several locations, including any offsite locations, such as alternate processing sites or storage facilities for backup data. Sample contingency plans may be obtained from the local ISSC.

f. Step 6. Testing and Revising Strategy. A contingency plan should be tested to train personnel and to keep the plan in step with changes to the environment. The extent and frequency of testing will vary among organizations and systems. There are several types of testing:

(1) Review. This is a simple test to check the accuracy of the contingency plan documentation. For instance, a reviewer can check the accuracy of contact telephone numbers, building and room numbers, and whether the listed individuals are still in the organization.

(2) Analysis. An analysis may be performed on the entire plan or parts of it. The analyst may mentally follow the strategies in the contingency plan and look for flaws in the logic or process used by the plan's developers. The analyst may also interview functional managers, resource managers, and their staff to detect missing or unworkable pieces of the plan.

(3) Disaster Simulations. These tests supply valuable information about flaws in the contingency plan and provide practice for a real emergency. While they can be expensive, these tests can also provide critical information for ensuring the continuity of important functions. In general, the more critical the functions and resources addressed in the contingency plan, the more it is cost-beneficial to perform disaster simulation.

(a) Report. Regardless of the type of testing performed, documentation of the test must be forwarded to the local ISSC and maintained on file within the organization until the local ISSC reviews the documentation during the regularly scheduled organizational security compliance review.

(b) Updates and maintenance. Because the plan will become dated as time passes and resources change, responsibility for keeping the contingency plan current should be

specifically assigned. Maintenance of the contingency plan can be incorporated into procedures for change management so that upgrades to hardware and software are reflected in the plan.

255 - 299. RESERVED.

CHAPTER 3. INFORMATION SYSTEMS SECURITY IN THE ACQUISITION PROCESS

300. PURPOSE. Many FAA systems are procured in full or in part. To ensure that the appropriate security measures are built into the system or component, the acquisition process must address system security needs. Appendix 6 describes the security activities performed throughout the acquisition process.

301-399. RESERVED.

CHAPTER 4. CONFIGURATION MANAGEMENT

400. PURPOSE.

a. Configuration management (CM) is an excellent information security tool. It consists of identifying, controlling, accounting for, and auditing all changes made to an information system during its complete life cycle. If an information system is under CM, as required by FAA Order 1800.8, National Airspace System Configuration Management, the required review of every proposed change provides an opportunity for analyzing its effect on the system's security; the resulting documentation provides assurance that all modifications to the system have been reviewed and approved by the system certifier. When the system certifier determines the modifications to be major, recertification and reauthorization shall be performed.

b. If a security compliance review of the system reveals modifications after authorization, a report shall be sent to the DAA from the ISSC. The DAA may shut down the system based on the findings in the report and initiate corrective action.

401. SYSTEM SECURITY LIBRARY.

a. There shall be a system security library for every FAA IS. The library shall contain all documents pertaining to the system's secure development and operation. This library may be part of a larger existing system library containing all documents, software, and other elements relevant to the information system. Each of the items listed below must exist in the library either as a separate and identifiable document, or, if the item is included in a larger document, it must be explicitly and completely cited by page and /or paragraph numbers.

(1) Master copy of the information system software

(2) Review document for ARs.

(3) Funding authorizations from the JRC.

(4) ISS plan.

(5) Inventory of all hardware to be operationally used (including firewalls and other perimeter protection devices), internal configuration (e.g., random access memory, disk size, cycle speed of the central processing unit), source and means of acquisition, and maintenance logs.

(6) Inventory of all software, GOTS and COTS software, the source and means of acquisition, and the current level or version.

(7) Licenses and copyright information for all system elements, including all codes or keys necessary to install the vendors software.

(8) Copies of all tradeoff studies performed during development.

(9) System requirements document.

(10) Top-level and intermediate-level specifications and developer produced documentation.

(11) Test procedures and results.

(12) Security test procedures and results.

(13) Interface agreements and supporting documentation, including memoranda of agreement (MOA), memoranda of understanding (MOU) and other formal or informal operating agreements.

(14) User manuals and operating instructions.

(15) Supervisor and administrator manuals.

(16) Site operating procedures.

(17) Operational contingency plan.

(18) All past and present certifications and authorizations, as well as copies of current certifications and authorizations for the system to which this system is interconnected.

(19) Reports of all security incidents pertaining to this system.

(20) All national change proposals submitted for the information system, as well as the results of their reviews (i.e., documentation of their acceptance or rejection).

(21) System's Configuration Management (CM) plan.

(22) Results of the system's physical configuration audit and functional configuration audit.

(23) Additional documents (e.g., concept of operations) that are relevant to the system's security.

(24) A list of all applicable Federal and contractor support personnel Points of Contacts (POCs).

(25) A copy of all maintenance and support contracts for all applicable hardware, and software products, including OEM and vendor contacts.

(26) A copy of all systems support contracts for applicable networks, systems, etc,

(27) Any other materials requested by the certifier or DAA and used in a certification and/or authorization.

b. Although many of these documents do not explicitly address information security, all are relevant to understanding an information system's security posture.

c. The system security library may be owned and managed by the system's designated CM personnel.

d. The system security library shall include the current versions of all documentation, as well as the versions of all security-relevant documents used for certification and authorization during the system's life cycle. Previous versions of other materials in the system library may be kept at the discretion of the system's manager.

e. Access to all system libraries, no matter the physical location, shall be restricted to FAA employees (including FAA IS security specialists assigned to the SSE) and contractors assigned to work on an IS.

402. HARDCOPY RECORD MANAGEMENT. Hardcopy records containing sensitive data will be managed in accordance with Appendix 8 of this Order, if applicable, and the following FAA Orders:

a. FAA Order 1350.14, Record Management

b. FAA Order 1350.15, Record Organization, Transfer, and Destruction

c. FAA Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information

d. FAA Order 1600.8, Communications Security (COMSEC) and Electronic Key Management Systems (EKMS)

e. FAA Order 1280.1, Protecting Privacy of Information About Individuals

403. SOFTCOPY RECORD AND DATA MANAGEMENT.

a. All removable media shall be clearly labeled regarding the required level of protection (see Appendix 8 of this Order for references).

b. Records management shall indicate whether softcopy files containing the records involved have been destroyed according to the required procedures for decommissioning (see Appendix 8 of this Order for references).

404. SECURE DISTRIBUTION.

a. The CM personnel for each NAS information system must establish procedures for securely distributing their system software to sites. The procedures for secure distribution shall be approved by the ISS Division manager or a designee.

b. A system control and distribution facility shall be provided for maintaining the integrity of the mapping between the master data describing the current version of the system software and the onsite master copy of the code for the current version. This facility shall be under the control of the program's CM personnel. Access to this facility must be limited to a small number of authorized individuals. Procedures (e.g., paper labels and receipts, software version IDs, distribution by registered mail, cryptographic wrappers) shall be used to ensure that the system software, firmware, and hardware updates distributed to each facility are exactly the same as the master copies. Appendix 8 provides additional guidance on transporting FOUO items.

c. Software distributed by electronic means must be protected against modification. These protection mechanisms (e.g., encryption of software, cryptographic wrappers) must be demonstrated and tested as part of certification and authorization testing.

d. Electronic distribution of information system software within the FAA is prohibited unless specifically authorized as part of the security plan package.

e. All software products or patches that are acquired electronically (e.g., from a vendor Internet site) and that are intended for inclusion as part of the system software of an operational system or as a tool to be used on an operational system must be identified to the certifier before the start of certification testing.

405 - 499. RESERVED.

CHAPTER 5. SECURITY MANAGEMENT AND ADMINISTRATION

500. WARNING BANNERS.

a. FAA information systems shall display an approved warning banner to each user prior to login. The warning banner must read:

WARNING: This is an U. S. Government protected computer system. Only authorized users performing authorized activities may use this system. Anyone using this system is subject to having their activities intercepted, monitored, recorded, captured, audited, and disclosed. Anyone's activities may be intercepted, monitored, recorded, captured, audited, or disclosed in any manner by authorized personnel, while reviewing the activities of other users. Anyone using this system consents to such interception, monitoring, recording, capturing, auditing, and disclosure, for any lawful purpose. All information, obtained or disclosed by any of the above methods, can be used as evidence for administrative or civil action, and/or criminal prosecution.

b. If an information system with remote access is a NAS system or connected to the NAS, the following terminology will be used in the warning:

WARNING: This is an U. S. Government protected computer system. Loss of human life may result from service interruption. Only authorized users performing authorized activities may use this system. Anyone using this system is subject to having their activities intercepted, monitored, recorded, captured, audited, and disclosed. Anyone's activities may be intercepted, monitored, recorded, captured, audited, or disclosed in any manner by authorized personnel, while reviewing the activities of other users. Anyone using this system consents to such interception, monitoring, recording, capturing, auditing, and disclosure, for any lawful purpose. All information, obtained or disclosed by any of the above methods, can be used as evidence for administrative or civil action, and/or criminal prosecution.

Paragraph 500 a. and b. also applies to FAA-owned laptops, notebooks, other portable equipment and non-FAA facilities. Additional information may be found in Appendix 7, Physical Security of IS.

c. FAA employees and contractors are encouraged to use of the Intranet and Internet for authorized use in their daily job functions. To remind employees and contractors that they are moving from the FAA Intranet to the open Internet, a warning banner or dialog box shall be displayed indicating the transition when feasible.

501. MANAGEMENT OF ACCESS CONTROL.

a. Access is the ability to do something (e.g., view or change) with or to a computer resource (program or data). Logical access controls are the means by which that ability is enabled, restricted, or denied. Such controls should be chosen and implemented based on the security level of the resources being protected. These controls may also serve to link access to an information system to specific individuals, where that accountability linkage is part of the applicable security policy.

b. Access to FAA information systems shall be controlled based on one or more of the following, as appropriate and, if the requesting organization or individual is from outside of the FAA, a memorandum of agreement or understanding (MOA/MOU) will be submitted. See FAA Order 1200.22C for guidance concerning the release of air traffic data to non-government entities.

(1) Identity of the individual, organization or process requesting the access.

(2) Type of action (view, change, delete, execute) sought.

(3) Object (information or program) to which access is desired.

c. Access to FAA information systems may also be restricted by other factors in effect at the time access is requested. These factors include:

(1) Role (job assignment or function) of the person requesting access. An individual may be assigned to one or more roles.

(2) Time (time of day and day of week) when access is requested.

(3) Physical or logical location from which the request for access is generated.

d. Access control criteria and administrative procedures to limit access to the information processed, stored, or transmitted by FAA systems shall be defined. These activities must be documented in the system's approved ISS plan, as discussed in Chapter 2, section 4. The activities should include at least the following:

(1) The access control criteria shall identify who is authorized access and who is responsible for approving it. This information shall be kept current.

(2) Access shall be controlled, not only to the programs that directly affect FAA operations, but also to those that can help penetrate (such as disk examination utilities) or damage (such as file defragmenters) the system. Similarly, the data to be protected shall include not only files that are critical for FAA operations, but also those files, containing user IDs and passwords, that are instrumental in protecting the operational files.

(3) The individual who requires access shall be appropriately briefed and shall possess appropriate authorization and a valid, operational need to know.

(4) The access granted shall be limited to that needed for the scope of the job or assignment.

(5) Unbriefed users shall be denied access to the information system.

(6) Personnel who become risks to security, or no longer have a valid need for access, shall have their access privileges removed promptly.

e. The identity of the access requester shall be verified (authenticated) by a combination of a user ID and one of the following:

(1) Password known to the individual.

(2) Token (a device such as a smart card) possessed by the individual.

(3) A characteristic (a biometric such as a fingerprint or retinal pattern) unique to the individual.

f. The applicable program office shall determine the elements to be used. Each method has advantages and problems. Passwords may be learned or guessed; tokens may be stolen or counterfeited. Users may forget passwords or lose tokens, and the administrative overhead for keeping track of the relevant data and tokens may be significant. Biometric systems may also have significant technical and user acceptance problems.

g. In new systems or existing ones where an authentication capability is to be added, the selection of an authentication method should be justified on the basis of its contribution to security versus the cost of using it. In particular, the justification for using passwords should be carefully examined; other forms of authentication may be preferable.

h. Access controls, user IDs, and passwords protect the system from unauthorized usage; therefore, it is important to manage them securely.

(1) User IDs that are inactive for a specified period of time (e.g., 90 days) shall be disabled.

(2) User IDs belonging to individuals who are no longer valid system users must be removed from the system.

(3) When passwords are used, they shall be defined, generated, and managed in accordance with the medium protection requirements of FIPS PUB 112. (See par 700(d)).

(4) In systems that use password authentication, users shall be required to change their passwords in accordance with the IS security level (see Chapter 2) as follows:

(a) Security level CS1 IS shall require password changes at least every 180 days.

(b) Security level CS2 IS shall require password changes at least every 90 days.

(c) Security level CS3 IS shall require password changes at least every 60 days.

(5) Suitable software should be employed for managing access controls to improve efficiency and reduce errors.

i. Access to sensitive data files may be further protected by encrypting the files. Like user authentication, cryptographic keys may be known to the individual; installed on a device possessed by the individual; or derived from a biometric.

j. If a private-key approach to encryption is used, the means by which cryptographic keys are distributed shall be carefully controlled. For example, a central key-issuing authority or a hierarchical structure of such authorities should be used. As an obvious target for penetration, the central authority or set of authorities must then be very well protected.

k. If a means of access (e.g., a password or encryption key) to a system is known or suspected to be lost or compromised, it must be changed promptly at both the system and user sides. Similarly, passwords and encryption keys should be revoked or invalidated promptly when individuals change roles or end their employment.

l. At a minimum, an annual re-certification of mainframe user-Ids shall be performed. This includes verification of:

(1) locator information (employee/contractor name, phone number, routing symbol, supervisor name and phone number, contract number and COTR (if applicable))

(2) access privileges are limited to that needed for performance of assigned duties.

502. PERIMETER CONTROL DEVICE ADMINISTRATION.

a. Perimeter control devices encompass devices such as firewalls, gateways, and routers

b. System integrity checks, such as tamper detection checks, of the network perimeter access control systems shall be performed on a daily basis. Audit logs from the perimeter access control systems and audit logs for servers and hosts on the internal, protected network shall be reviewed daily.

c. All perimeter control administration shall be performed from the local, dedicated terminal. No access to the perimeter control operating software shall be permitted through remote access unless explicit approval is granted by the DAA and adequate security controls, such as a Virtual Private Network (VPN), are in place. Physical access to the system terminal shall be limited to the administrator and backup administrator(s); all visitors must be under escort. Physical access to the device must be tightly controlled to preclude any unauthorized changes to the configuration or operational status, and to eliminate any potential for activity by a monitoring device. In addition, precautions should be taken to ensure that proper environment alarms and backup systems are available to ensure the device remains online. Consideration should be given to providing remote alarm notification to administrators during off hours. The perimeter control device software must not be corrupted by running on a shared computer; all non-device related software, such as compilers, editors, communications software, shall be deleted or

disabled. Commercial products that host perimeter control device software with other applications shall be reviewed on a risk-benefit basis. ISS Division and DAA approvals are required for such products. New services shall be implemented after the risk-benefit analysis.

d. The operational procedures for a perimeter control device and its configurable parameters must be well documented, updated, and secured. This ensures that if an administrator resigns or is otherwise unavailable, an experienced individual can read the documentation and rapidly assume the administration of the device. In the event of a system break-in, such documentation is needed for re-creating the events that caused the security incident, and for investigative purposes during a criminal investigation. Backup copies of software and documentation shall be kept in suitable, secure, offsite storage.

e. To ensure security is maintained on all perimeter control device, the following must be followed:

(1) systems administrator shall maintain an awareness of all required system or component hardware and software upgrades

(2) all vendor recommendations for processor, memory capacities, new releases of the system software, and security patches shall be applied to the systems in a timely manor

(3) hardware and software components shall be obtained from vendor-recommended sources

(4) during the upgrade process, the system must provide the same level of security, through a redundant system or some other means to prevent unauthorized access

(5) after the upgrade process is complete, all perimeter control devices shall be tested to verify proper operation

(6) vulnerabilities learned by the ISS Division will be forwarded to system owners through the alert notification process, described in chapter 11

(7) systems administrator shall implement ISS Division recommendations in a timely manner

f. Procedures should be developed for reconfiguration or maintenance to ensure that no vulnerabilities are introduced to the system during the process.

g. The perimeter control devices shall enforce a defined security policy configured to deny all services not expressly permitted.

h. Strict control of modem access via direct dial-up lines into the network shall be maintained. Existing dial-up network access must be approved as specified in Chapter 2, par 234. Dial-up access must be re-certified annually (excluding modem pools). The DAA may not delegate the authority to permit or deny dial-up access.

i. Perimeter control device administrators shall be properly trained and experienced with the perimeter control device and the operating system of the platform on which it operates. Administrators must maintain awareness of changes and recommendations for their specific perimeter control device, as well as for the general class of such devices, through such mechanisms as vendor and general WWW sites and groups.

503. SECURITY REVIEW OF NEW AND CHANGING NETWORK APPLICATIONS. With ever-changing technology, new network applications are constantly being made commercially available. It is essential that a complete security review of such applications be made prior to their use within the FAA to prevent the introduction of security weaknesses into FAA networks. This review is an integral part of CM for the information system. New network applications must be approved by the DAA.

504 - 599. RESERVED.

CHAPTER 6. NETWORK AND INFORMATION SYSTEMS SECURITY

600. CONNECTIONS BETWEEN INFORMATION SYSTEMS.

a. Connections between information systems, whether using public or private communications media, must be approved by the DAA to ensure that adequate information protection is in place. Because of the rapid pace of technological development, no design, testing, or operational assumptions should be made based solely on whether a public or a private communications medium is used.

b. The Certification Authority and the DAA will jointly ensure that appropriate safeguards, are in place, based on the sensitivity of the information. Documentation (e.g., license agreements, interconnection agreements) are executed on behalf of the FAA as part of the approval process. These licenses and agreements shall be under configuration management (CM) control.

601. ENCRYPTION.

Encryption may be employed to protect information when such protection is deemed necessary and approved by the DAA. FIPS 140-1, Security Requirements for Cryptographic Modules, from NIST has been designated as the Federal Government standard for encryption. Only products from the NIST-approved validation list shall be used in the FAA. The following documents are supporting publications for encryption and key management.

(1) FIPS 46-2 and 81: Data Encryption Standard (DES) and DES Modes of Operation.

(2) FIPS 186 and 180-1: Digital Signature Standard (DSS) and Secure Hash Standard (SHS).

(3) FIPS 113: Computer Data Authentication, which specifies the generation of a *Message Authentication Code (MAC)*, from ANSI X9.9.

(4) FIPS 171: Key Management Using ANSI X9.17.

602. INTERNET SERVICES.

a. FAA Order 1370.79, Internet Policy, establishes FAA policy on the use of the Internet, or similar electronic communications media.

b. Any access to Internet services from an FAA information system must satisfy two conditions.

(1) First, approval to connect to the Internet shall be obtained in writing from the DAA. A copy of each signed approval shall be maintained by the division or LOB of the requestor. Contractor approvals shall be maintained by the CO for the contract. For IS requests, a copy will also be part of the security plan package.

(2) Secondly, access shall be via an approved boundary protection gateway (e.g., screening routers, firewalls) that has been approved by the DAA of the ISS being protected.

c. Service providers, either directly connected or dial-up, shall not be used to access the Internet, unless such connection is approved by the DAA. Although the configuration of some networks make it technically possible to access the Internet without going through an approved gateway, such access is prohibited.

d. All exceptions must be approved in writing by the Associate Administrator for Civil Aviation Security.

603. NETWORK MANAGEMENT TOOLS.

a. Network Management protocols. Network management protocols are used to provide information about the health of FAA networks and the devices attached to the network. Network management protocols can be used to collect statistics about the network, determine trends on the

network, make changes to device configurations and even reboot or power off devices. The protection of these protocols from unauthorized use is extremely critical.

b. Network Analyzer Tools. Network analyzer tools are used to troubleshoot and track down problems on networks. It allows LAN and network administrators to look at the packets of data on the network. Network analyzers come in many forms. They may be a standalone portable tool meant to be taken from one network to another, a tool meant to be placed permanently on the network and monitored from another workstation, or may be an application software package running on a PC or UNIX workstation. Many network analyzer tools have features which can generate traffic on the network, usually to simulate a load on the network. These tools are indispensable for finding network problems, but if misused, can affect network performance or corrupt or disrupt network services. To meet legal requirements, the appropriate warning banners discussed in paragraph 501 must be in place prior to using these tools on an FAA system.

(1) Securing Network Analyzer Tools. Because network analyzer tools are so powerful, they must be secured at all times.

(a) Standalone, portable tools should be locked in a secure location when not in use.

(b) Network analyzer tools which have been installed (permanently or temporarily) on the network must ensure that the device is secure from unauthorized access or use.

(c) Hardware level passwords must be enabled in the firmware of all network analyzer devices to prevent access by rebooting the analyzer.

(d) Application level or screen saver passwords must be enabled when the analyzer is operating in an unattended mode.

(e) The use of SLIP connections to the analyzer devices should be limited and tightly controlled by the network administrator.

(f) If application level passwords or screen saver passwords are not implemented on the analyzer, then other precautions must be taken to ensure that tampering with the device cannot occur. Removal of the keyboard, placing the analyzer in a locked environment, or in an area which is monitored during the operation of the analyzer (such as a help desk area), should be considered.

(3) Use Logs. Owners of network analyzer tools should maintain logs of use.

(4) Knowledgeable Users. Users of network analyzers must thoroughly know and understand the tools they are using so they do not disrupt network services.

(5) Handling of Network Traffic Packets Captured by an Analyzer. The purpose of the network analyzer tools is to capture network traffic to allow analysis of what the network is doing. Because the information contained in the packets may contain sensitive data, care must be exercised in handling of captured packets.

(a) If it is necessary to send copies of the packet captures to another source (vendor) for additional analysis, then care must be taken when transmitting the data. The data may be copied to removable media and mailed, but under no circumstance should the file be sent over the Internet without encryption.

(b) Captured packets, which are no longer required, should be deleted from the system.

(c) Captured packets which must be maintained, must be protected just as any other sensitive information. Paper copies must be marked appropriately.

604. SPECIALIZED COMMUNICATIONS.

a. Facsimile. Information transmitted via fax shall be protected commensurate with its sensitivity. Instructions for sensitive security information are in Appendix 8 of this Order.

b. Telephony Systems.

(1) Sensitive information transmitted via telephonic systems, including the public switched telephone network, Private Branch Exchanges (PBX), and voice mail systems, shall be protected by a protection mechanism (e.g., encryption) that has been approved by the DAA. Instructions for sensitive security information are in Appendix 8 of this Order.

(2) Unprotected telephonic systems are susceptible to unauthorized access. Messages should not be left on a voice mail system that, if compromised, could damage the FAA's mission. Suspected, unauthorized access attempts shall be promptly reported to the servicing security element (SSE) and others as specified by individual lines of business.

(3) PBX, voice mail, cellular telephones, pagers, and voice interactive response systems must be physically secured and system security features configured (to the extent possible and practical for a specific system) to prevent unauthorized access to dial tones or modems and to prevent other unauthorized access to the information system.

(4) Any access to telephonic services from an FAA information system must be via protection devices that have been approved by the DAA. The ISS Division can provide guidance and product recommendations. In general, modems shall be protected against unrestricted access. Connections made via modems shall be subject to an authentication challenge.

(5) Presently, separate voice, video, and data networks are used at the FAA. New technology exists to allow voice, video and data to be carried over the same physical network infrastructure. Any implementation of this new technology must consider integrity, reliability, accuracy, timelines and security of telephonic data. Employees should consult FAA Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information for guidance on systems handling these types of information.

(a) Audio Teleconferencing. Audio teleconferencing can be an economical method of holding a meeting between participants from various locations, it cuts travel costs, and reduces loss of productivity due to travel time of the participants. However, care must be used when discussing sensitive issues.

(b) Video Teleconferencing. Video teleconferencing is also currently being used within the FAA, and is available in every region and center. Video teleconferencing is also an economical method of holding a meeting between participants from various locations, it cuts travel costs, and reduces loss of productivity due to travel time of the participants and adds the benefit of seeing all the participants. Just as with an audio teleconference, care must be used when discussing sensitive issues.

c. Electronic Mail. Sensitive information transmitted via electronic mail (e-mail) shall be protected by a suitable mechanism (e.g., encryption). Information transmitted via e-mail shall be protected commensurate with its sensitivity, both in softcopy and hardcopy form. Instructions for sensitive security information are in Appendix 8 of this Order.

(1) Mail going over the Internet uses Simple Mail Transfer Protocol (SMTP) which is a clear text scheme for transmission of the mail message. Messages sent using SMTP can be read by anyone, which presents a security vulnerability if sensitive FAA information is sent. Organizations should establish an internal policy regarding the protections required for its sensitive data being transmitted.

(2) As stated in paragraph 602, it is the FAA policy that Internet access shall be via an approved boundary protection gateway (e.g., screening routers, and firewalls) that has been approved by the DAA. Therefore, unless a specific authority is granted by the DAA, FAA users may not use electronic mail accounts with local Internet Service Providers (ISPs) to conduct FAA business. This type of usage presents a security vulnerability when outside providers are used to store and transmit sensitive FAA information. Agency provided electronic mail accounts should be utilized.

605. VIRTUAL PRIVATE NETWORK.

a. A Virtual Private Network is a set of communications facilities that are intended to function as a private (i.e. isolated) communications network, even though they use the same protocols as, and possibly are connected to, public backbone network systems such as the switched telephone network or the Internet. When properly designed, configured and maintained, a VPN can provide some assurance that network traffic among FAA sites is protected against unauthorized disclosure and modification. Regardless of VPN protections that may be provided, any interconnection with public networks is still subject to the appropriate portion of this policy regarding those public networks.

b. A boundary is any software, hardware, or physical barrier that limits access to a system or part of a system. A security boundary indicates the demarcation between a set of information systems that are protected by the system security mechanisms; anything outside the boundary is either unprotected or, more generally, protected by a different security policy. The VPN shall employ boundary protection (e.g., firewall-to-firewall encryption) to provide services such as, but not limited to:

(1) Encryption/decryption.

(2) Strong authentication for non-FAA nodes and dial-in.

c. The VPN shall support interoperability standards such as the most recent versions of:

(1) Internet Engineering Task Force (IETF) Request for Comments (RFC) 1825-1829, commonly known as the Internet Protocol Security (IPSEC) standards.

(2) Rivest, Shamir, and Adelman (RSA) Secure/Wide Area Network (WAN) (S/WAN) initiative.

d. The VPN shall support the implementation of various encryption algorithms in addition to those provided by the product vendor. The FAA shall use only those encryption algorithms approved for use by Federal government agencies (see paragraph 601).

606. NETWORK-BASED INTRUSION DETECTION.

a. Intrusion detection systems (IDSs) are predicated on the assumption that an intruder can be detected through an examination of various parameters such as network traffic, central processing unit use, input/output, user location, and various file activities. System monitors, called daemons on UNIX® systems, convert observed parameters into chronologically sorted records of system activities. Also known as audit trails or intrusion logs, these records are analyzed by IDSs for unusual or suspect behavior. IDSs may use either rule-based or statistics-based approaches. IDSs designed to protect networks typically monitor network activity; IDSs designed for single hosts typically monitor operating system activity. All information systems with audit trail capability must implement the feature. The level of auditing will be determined by the findings of the system risk assessment. Audit trail data must be maintained a minimum of 90 days.

b. Network-based intrusion detection (NBID) complements the operating system-based intrusion detection incorporated in the audit requirements (see Chapter 7). NBID examines communications traffic and protocol elements to identify potential violations of security policy. Each line of business shall determine the conditions requiring a NBID.

c. NBID shall include a capability to detect and respond to potential or suspected network-based intrusion. This capability must be kept current with the constantly evolving state-of-the art intrusion threats and countermeasures. NBID shall provide the following features (consistent with the state-of-the art):

(1) Recognition of known, malicious communications based on indicators such as patterns, sequences, connections, and network addresses.

(2) Ability to accept descriptions of intrusion indicators.

d. NBID shall configure for automatic and manual operation, and provide:

(1) Real-time intrusion detection.

(2) Real-time reaction to detected intrusions, including optional responses selected by the DAA and included in the Computer Security Incident Response Capability (CSIRC) Concept of Operations, to terminate a connection, log out a user, or shut down a component [e.g., NAS or operational support system].

(3) Real-time alarms for detected intrusions, including optional responses selected by the DAA to employ pagers and e-mail.

607 - 699. RESERVED.

CHAPTER 7. INFORMATION PROTECTION RESPONSIBILITIES

700. SYSTEM IDENTIFIERS AND AUTHENTICATORS.

a. User Responsibilities. Users shall be responsible for safeguarding system identifiers and authenticators, such as user IDs and passwords, which are assigned to them. Neither user identifiers nor authenticators may be shared with other users.

b. Systems, LAN, and Network Administrators Responsibilities. Systems, LAN, and Network administrators are responsible for protecting root level passwords on network devices which are in their control. They are also responsible for implementing system controls that require use of good passwords (to the extent supported by the operating system) and regular password changes based on the requirements of the system's CS level.

c. Logging Access. All successful and unsuccessful attempts to log on to all FAA networks or systems shall be logged automatically to an appropriate log file by the systems logon process. The log files must be retained for a minimum of 90 days.

d. Creation and handling of passwords. Users shall be responsible for following password configuration procedure, for changing passwords as required, and for ensuring the security of their passwords. Unless incompatibility with other technical protective measures is shown, where password capability is provided, passwords shall be used to make unauthorized access more difficult.

(1) Password configuration. User level passwords must follow established FAA criteria. For further guidance, see FIPS PUB 112, Standard Password Usage. In general, passwords:

- must not be words that appear in the dictionary
- must not indicate personal information, such as a spouse or child's name, birthday, etc.
- must not be written down, embedded in script files, or displayed in a prominent location
- must be changed at least every 60 days for IS of security level CS3
- must be changed at least every 90 days for IS of security level CS2
- must be changed at least every 180 days for IS of security level CS1
- must include at least one numeric or special character
- must be at least 6 characters long.

Even though a unique user ID is required for each user, the system may allow more than one user to have the same password. In such cases, the system must accept the passwords without revealing that they have been used by others and must not reveal the IDs of any other users that selected the same password.

(2) Default Accounts and Passwords. Many systems, and applications come with one or more default system accounts and passwords (or no password) setup to make the installation of the system easy for novice users.

(a) All default accounts must be removed from the system, or the default password must be changed prior to placement of the system or device in to service.

(b) All system or root level accounts shall have a password assigned prior to placement of the system or device in to service. Accounts with this level of access must be kept to a minimum.

(c) All "guest" accounts must be removed from the system or must have a password setup to gain access to the system or device.

(d) All new user accounts must have a password assigned to them.

e. Management Access. Identifiers and authenticators to FAA systems are provided in order to protect sensitive information from unauthorized use or viewing. Such protections are not intended to prevent appropriate review by FAA management. Consistent with the warning banners and appropriate training referenced in Chapters 5 and 8, FAA management reserves the right to monitor employees' use of any information system without any additional notification.

701. SOFTWARE COPYRIGHT PROTECTIONS.

a. Title 17 USC, Section 106, gives copyright owners exclusive rights to reproduce and distribute their material, and section 504 states that copyright infringers can be held liable for damages to the copyright owner. Title 18 USC, provides felony penalties for infringing on a software copyright. Copyright agreements will be honored.

b. FAA employees and contractors shall also be responsible for ensuring that software is properly licensed before being installed on FAA equipment.

c. FAA employees and contractors will keep a copy of the legal license in the work area for any authorized personal software used on FAA information systems and will be available to FAA ISS specialists for inspection.

d. Organizations, which distribute or provide users access to applications over the network, must provide sufficient number of license for all concurrent users of each application. Each organization must also ensure that the maximum number of licenses is not exceeded.

e. Shareware and freeware must be reviewed and approved by the ISSO prior to installation. All usage must be in compliance with copyright and security requirements.

702. PROTECTIONS AGAINST MALICIOUS CODE. The National Information Infrastructure Act of 1996, which amends 18 USC 1030, states that to willfully introduce malicious code into a U.S. Government system can be a criminal offense. Therefore, it is incumbent on the FAA to introduce procedures to protect information systems against the introduction of malicious code into the FAA infrastructure, an integral part of the national critical information infrastructure. Written procedures must be put in place by each line of business for users to follow. Malicious software, such as viruses and Trojan horses, represents an increasingly serious security and integrity problem for information systems. This software has the capability to disrupt operations and destroy or alter data. FAA users shall follow these guidelines to protect their systems:

a. Information system users shall use malicious code protection software to prevent, detect, and eradicate malicious code.

b. Files downloaded from another system shall be scanned immediately for malicious code.

c. Diskettes received from another user or organization as well as shrink-wrapped diskettes shall be scanned for malicious code prior to use.

d. Files attached to e-mail messages will be scanned prior to opening the attachments.

e. Individuals discovering malicious code on any media will report the discovery to the assigned ISSO, who will report the discovery to the SSE on the FAA-approved incident report form in Appendix 3 of this Order. Multiple occurrences within a short timeframe may be consolidated for incident reporting purposes. A copy of the incident report will be sent to the ISSM and ISSD only if the malicious code proves destructive or invasive. A consolidated report of malicious code incidents will be forwarded by the ISSC to the ISSD every 6 months of the calendar year and due February 15 and July 15.

703. PROTECTION OF SYSTEMS.

a. Government-owned/leased information systems, whether accessed from the worksite or remotely, shall be used only to conduct official Government business. Violation of this requirement may

result in disciplinary action in accordance with Agency guidelines. For further information, see the Federal Aviation Personnel Manual (FAPM) 2635, Conduct and Discipline.

b. Cracking passwords and breaking into accounts are categorized as malicious activities. As such, these activities must be confined to formal penetration testing and are governed by the requirements in Chapter 10.

c. Disruption of FAA information system service and abuse or misuse of an information systems or tools are not permitted. Such actions may result in administrative, civil or criminal actions.

d. Incidents of loss, theft, or damage to computer equipment shall be reported immediately to the ISSO, who will complete the FAA Form 4630-8, Report of Survey, and forward it to the servicing security element (SSE). Incidents of system misuse, damage to software or data, and lost/theft/damage of equipment shall be handled and reported in accordance with the procedures specified in Chapter 10 using the FAA-approved incident reporting form in Appendix 3 of this Order. In addition, a separate statement reporting the impact of loss of the data will be sent to the SSE on the approved FAA incident report form.

e. Information systems shall not be placed in areas that do not have basic physical access controls (e.g., locks on doors). Standard FAA procedures for protection of pilferable items shall be followed. For further guidance, see FAA Order 1600.6, FAA Physical Security Management Program and Appendix 7 of this Order.

704. PROTECTION OF INFORMATION. OMB Circular A-130 states that all U.S. Government information systems contain some sensitive information.

a. The FAA processes many types of information, much of which is mission critical. For information categories, see Chapter 2. Users of FAA information systems shall adhere to all system security requirements defined in the ISS plan to ensure the confidentiality, integrity, and availability of information.

b. Users should make every effort to protect monitor screens, printers, and other devices with human-readable output from the view of casual observers or passersby. This protection shall be achieved by using a password protected screensaver if the capability is available. Other means of protection may be provided by exiting the application, locking the office area, or logging off the system before leaving the area.

705. MARKINGS. Markings on all hardcopy sensitive data and removable media containing sensitive data shall include the identity and organization of the information owner, the date the marking was applied, the security level of the data, and any additional restrictions. Human-readable markings are always required on the media (e.g., on the diskette label). Markings shall also be associated with the information itself whenever it is in human-readable form. See Appendix 8 for markings of FOUO and SSI.

706. PROTECTION REQUIREMENTS FOR INFORMATION. The U.S collaborated with other countries on the successor to the NSA Rainbow Series for information technology. The result is the ISO/IEC 15408-1 “Information Technology – Security Techniques – Evaluation Criteria for IT Security”. In November 1998, the FAA signed an agreement to use this standard. With the publication of this order, the FAA adopts the standard “common criteria”. The guidance that will be used is published by NIST.

707. USE OF PRIVATELY OWNED SYSTEMS AND SOFTWARE. Before an FAA employee or contractor uses a privately owned computer and/or software, on or off the work-site, to conduct Government business, permission must be granted in writing by the responsible FAA manager. The request should include justification, the period covered, the limitations affecting any Government-owned or privately-owned software, and the applications that will be accessed. All software usage must be in compliance with copyright restrictions. A copy of the requesting memo must be forwarded to the organizational ISS officer. See Appendix 3 for a sample memo. The use of privately owned systems and software must be addressed in the Information Systems Security Plan and system certification and authorization.

a. The FAA may permit employees (and contractors) to use privately owned microcomputers to work on Government business, subject to prior written approval by the organizational manager, and with controls over records, property, and personnel activity.

b. Records created, stored, and used on privately owned computers for official FAA business are the property of the Government and may be considered Agency records. The user agreement specifies protections that must be afforded the data, including those specified in, but not limited to, Chapter 7.

c. The FAA shall not assume any responsibility for the safety, maintenance, security, or operation of the software or equipment. The hardware, software, and data may be subject to unannounced inspection, as stated in the user agreement. A user's noncompliance with a request for an FAA inspection will be cause for immediately terminating the approval to process FAA data on the privately owned computer.

d. Managers and supervisors shall ensure that U. S. Government files and records created and used on privately owned computers for FAA activities will remain readable and accessible by the Government.

e. Use of FAA data and records shall be based on the agency's needs, not on the convenience to private individuals.

f. When an employee is terminated or leaves the government, or a contractors contract expires or is terminated, then:

- all FAA data and records must be turned over to the FAA
- all traces of the data and records must be removed from all privately own systems
- all copies of the data and records must be destroyed
- all FAA provided GOTS and COTS software must be removed from all privately owned systems

708. USE OF INTERNET OR SIMILAR ELECTRONIC COMMUNICATIONS MEDIA.

a. Users shall only use the FAA-provided Internet services, such as, but not limited to, the World Wide Web (WWW), Gopher, and WAIS, for performing their job function. Using FAA-provided Internet services for personal purposes is prohibited by FAA Order 1370.79, Internet Policy, and the Federal Aviation Personnel Manual 2635, Conduct and Discipline.

b. Internet usage shall be captured in log files. Log files and backups and may be used in support of administrative, civil or criminal actions. Interactive monitoring of an employee's usage may be authorized by the SSE.

c. Users are prohibited from knowingly and intentionally accessing, transmitting, or downloading material that is obscene, pornographic, threatening, treasonous, subversive, racially or sexually harassing, or otherwise illegal material as specified in applicable Federal law and regulations or in violation of any FAA orders and directives, including, but not limited to, the Conduct and Discipline FAPM Letter 2635.

d. Contraband is any data that it is a violation of Federal, state or local law to possess no matter what form the data takes. If contraband data is discovered on any FAA information system, the ISS Division and the FBI and will immediately be notified. All automated and manual documents, records, or automated media will be secured until the arrival of law enforcement authorities.

e. Users shall only access the Internet through an officially designated HTTP proxy server, Network Address Translation (NAT) server, or other approved access method. Regardless of the method used to access the Internet, all activity shall be logged.

f. Users shall scan downloaded files for viruses and other malicious content by using authorized, updated virus software in accordance with paragraph 702 of this Order.

709. ELECTRONIC MAIL (E-MAIL).

a. Use of E-Mail. Refer to FAA Order 1370.81, Electronic Mail Policy.

(1) E-mail is provided by the FAA for employees to conduct official business. Using e-mail for personal business is not allowed. E-mail shall not be used for partisan political endeavors, private fund raising, passing chain letters, etc.

(2) All electronic messages created and stored on FAA information systems are the property of the FAA and are not considered private. The FAA reserves the right to review all employee e-mail communications. E-mail messages may be retrieved by the FAA even though they have been deleted by the sender and the reader. Such messages may be used in administrative, civil or criminal actions.

(3) If sensitive or proprietary information must be sent by e-mail, users shall use password protection. Instructions for sensitive security information are in Appendix 8 of this Order and encryption is referenced in paragraph 600 of this Order.

(4) Users shall scan incoming messages for viruses and other malicious content by using authorized, updated virus software in accordance with Appendix 8 of this Order.

(5) Users shall not transmit sensitive information outside of the FAA intranet in clear text format (such as used with Internet mail). Instructions for sensitive security information are in Appendix 8 of this Order.

b. Retention of E-Mail Messages. The National Archives and Records Administration has issued standards for managing Federal records created on or received through e-mail. Employees shall familiarize themselves with the criteria for determining whether an e-mail message is a Federal record. The cognizant records management officer can provide guidance about retaining e-mail messages.

Table 7-1.

710 - 799. RESERVED.

CHAPTER 8. ISS AWARENESS, TRAINING, AND EDUCATION

800. PURPOSE.

a. ISS training teaches employees and contractors the skills that will enable them to perform their jobs more securely. Employees and contractors who understand their ISS responsibilities, the need for security, and the methods for ensuring it are among the best protections against computer security incidents. All managers and employees should be aware of the reasons for each security requirement to be followed or enforced. Each manager must know the general and specific security requirements for their particular area of responsibility.

b. The success or failure of the ISS plan depends, to a significant degree, upon the training provided to the employees who manage, provide, or use information systems. To ensure that all employees and managers acquire and maintain the skills and knowledge to discharge FAA ISSP responsibilities, each line of business shall include an ISS Training and Awareness Program.

801. ACCOUNTABILITY. Both the dissemination and the enforcement of policy are critical issues that are implemented and strengthened through training programs. Employees need to be accountable for following applicable FAA ISS policies and procedures in order to act effectively in securing information systems.

802. OBJECTIVE. The objective of ISS security training is to improve protection of FAA information systems and the security and privacy of sensitive information. Because human actions account for a far greater degree of computer-related loss than all other sources combined, the goal of the FAA ISS plan is to ensure that all personnel and contractors dealing with FAA information systems are provided adequate ISS training. Such training can reduce employee errors and omissions and by informing all employees about accountability and penalties for fraud and unauthorized activity. Training can also reduce such activities by disgruntled employees.

803. TRAINING DEVELOPMENT.

a. The ISS Division is responsible for establishing an ISS awareness and training process. This process includes providing guidance to each organization in establishing ISS awareness, training, and education. Further guidance in developing training for FAA employees and contractors can be found in the NIST Special Publication,800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*. The NIST publication segments training into six functional areas that represent categories of generic organizational roles: manage, acquire, design and develop, implement and operate, review and evaluate, and use. Because individuals acquire different roles within an organization over time, security training and education are to be provided selectively, based on an individual's particular job functions, responsibilities, and needs.

b. Each organization directly reporting to AOA-1 is responsible for developing a plan to ensure that employees are provided initial and recurrent ISS training and that all ISS training requirements are met. Each line of business shall forward a copy of their ISS training and education plan to the ISS Division for review and approval prior to its implementation. The ISS Division will review each plan to ensure consistency of training, guard against errors and omissions, and facilitate sharing of developed resources among lines of business to eliminate duplication of effort.

804. MINIMUM REQUIREMENTS FOR TRAINING.

a. This section establishes the minimum requirements for security awareness, training and education that must be provided to FAA employees and contractors.

(1) Executives shall receive awareness training in computer security basics, computer security policy and procedures, contingency planning, incident management, and systems life cycle management; and policy level training in security planning, and management.

(2) Program and functional managers shall receive awareness training in computer security basics; implementation level training in security planning and management, incident

management, and computer security policy and procedures; and performance level training in contingency planning and in systems life-cycle management.

(3) Information systems security personnel shall receive awareness training in computer security basics; and performance level training in security planning and management, incident reporting and handling procedures, computer security policies and procedures, contingency planning, and systems life-cycle management.

(4) Information system management and operation personnel shall receive awareness training in computer security basics; and performance level training in security planning and management, computer security policies and procedures, contingency planning, incident reporting and handling procedures, and systems life-cycle management.

(5) End users shall receive awareness training in computer security basics, security planning and management, and systems life-cycle management; and performance level training in computer security policies and procedures, contingency planning, and incident reporting.

b. The frequency of the training will be provided as follows:

(1) Initial training. New or reassigned employees must receive ISS training within 60 days of their appointment.

(2) Continuing training. Training shall be provided when there is a significant change in the information security environment or procedures or when an employee enters a new position that deals with sensitive information.

(3) Refresher training. Computer security refresher training shall be given as frequently as deemed necessary by the ISSM, based on the sensitivity of the information that the employee uses or processes. However, employees and contractors shall receive refresher training at least biennially.

805. TRAINING LEVELS. Training must focus on job functions, or roles and responsibilities specific to individuals, not on job titles. Training must recognize that individuals have unique backgrounds and, therefore, different levels of understanding. Individuals may have more than one organizational role and will need ISS training that satisfies the specific responsibilities of each role. The following are the stages of this training:

a. Awareness Programs. All FAA employees/contractors shall be provided with basic ISS concepts and procedures. The first approach is awareness, which is a precursor to ISS security training. ISS awareness eliminates redundancies across audience categories and establishes a baseline of FAA-wide ISS knowledge, which all employees can reasonably be expected to have as they change jobs. Awareness is NOT training. Security awareness is explicitly required for ALL employees and contractors in OMB Circular A-130. Awareness activities include security awareness video tapes, CDs, posters, flyers, software, Internet, and web sites.

b. Security Basics and Literacy. This transitional stage between awareness and training provides the foundation for subsequent training by presenting a universal baseline of key security terms and concepts. After this stage, training focuses on providing individuals with the knowledge, skills, and abilities specific to their ISS roles and responsibilities.

c. Training. ISS training provides the knowledge and skills that will enable employees to perform their jobs more effectively. Training strives to produce relevant and needed security skills and competency for practitioners of functional specialties other than ISS (e.g., management, systems design and development, acquisition, auditing). Training must provide practical instruction, for example, lectures and demonstrations, case studies, and hands-on-practice.

d. Professional Education. This ISS education is a separate learning level and is targeted for security professionals and those whose jobs require expertise in ISS. This education involves theoretical instruction (e.g., seminars and discussions, reading and study, and research). ISS education and associated on-the-job experience are important for ISS coordinators (ISSCs), ISS managers (ISSMs), and ISS officers (ISSOs) to fulfill their roles. Education integrates the security skills and competencies of the various

functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce ISS professionals capable of vision and proactive response.

806. TRAINING MATRIX. Table 8-1 shows the minimum level of training to be achieved in each subject area by each audience category. Different audience categories may be expected to reach the same training level, yet have different learning objectives for that level, because of different job functions.

807. TRAINING SUBJECT AREAS.

a. Computer Security Basics introduces basic concepts of computer security practices and the importance of protecting the information from any vulnerability to known threats.

b. Security Planning and Management covers the concept of all aspects of risk analysis, the determination of security requirements, the security training, and the internal agency organization to carry out the computer security function.

c. Computer Security Policy and Procedures presents Federal and DOT security practices in the areas of physical, personnel, software, communications, data, and administrative security.

d. Contingency Planning covers the concepts of all aspects of emergency planning, backup, response, and recovery. It identifies the roles and responsibilities of all personnel involved.

e. Systems Life-Cycle Management discusses the way security is addressed during each phase of a system's life cycle, from planning through operations and decommissioning.

Table 8-1. Training Matrix

Audience Category	Training Area Examples	Computer Security Basics	Security Planning and Management	Computer Security Policy and Procedures	Contingency Planning	Systems Life-Cycle Manage-ment
Executives	SES and FG-15s and FV-J/K	Awareness	Policy	Policy	Awareness	Awareness
Program and functional managers	IPTs, Division Mgrs, Program Managers	Awareness	Implementa-tion	Implementa-tion	Performance	Performance
IRM, security and audit	Region (IRMs) ISSC/ISSO/ ISSM	Awareness	Performance	Performance	Performance	Performance
ADP management and operations	Computer and related Series (e.g., FG-334s, 854s,2152s, Technical Job Category)	Awareness	Performance	Performance	Performance	Performance
End users	All FAA personnel	Awareness	Awareness	Performance	Awareness	Awareness
Contractors	All	Awareness	Performance	Performance	Performance	Performance

808. REPORTING. To measure the effectiveness of the training program, the ISSM for each line of business will provide a report on the number of Government employees and contractor personnel involved in the ISS Awareness, Training, and Education Program to the ISS Division. The report will include the

type of training provided and the projections for the next fiscal year. The report will be submitted to the ISS Division on November 30, for the previous fiscal year. The ISS division will furnish an information copy of the report to the ISSCs.

809. EVALUATION AND FEEDBACK. Training courses and materials should be evaluated periodically to assess suitability and to ensure that materials are kept current. Feedback about the training should be requested from each course participant. For instructor-led training, a questionnaire should seek feedback about the material and about the instructor's knowledge and presentation skills. Self-study material, such as video tapes, computer-based training, handbooks, and web pages, should include a feedback questionnaire, either built into the product or distributed with the material. At a minimum, the questionnaire should examine the audience's perception of the overall quality of the presentation, the completeness of the material, and the ease-of-use of the chosen presentation media. All feedback shall be reviewed and considered in the update of course materials and contents.

810 - 899. RESERVED.

CHAPTER 9. ISS PROGRAM AND COMPLIANCE REVIEWS

900. GENERAL. The ISSP ensures that organizations are following applicable policy by conducting independent inspections or reviews. There are two levels of reviews within the ISS Program.

a. ISS Program Reviews. These are inspections of the ISS Program managed by each SSE. These reviews are to ensure compliance with FAA Orders and policies and to collect information for evaluation of the ISS program for effectiveness and improvement. The program review inspections will be conducted by ISS specialists from the ISS Division.

b. IS Security Compliance Reviews. These are inspections conducted to examine whether the system is meeting stated or implied security requirements, including system and organizational policies stated in the security plan package. An ISSC or ISS Division specialist reviews controls in place and determines whether they are effective. Techniques used include inquiry, observation, and testing of the controls and the data. The inspection, which will include site inspection of FAA facilities or non-FAA facilities, can also detect illegal acts, errors, irregularities, or a lack of compliance with laws, regulations, policy, and contracts.

901. OBJECTIVE. ISS Program Reviews address records, logs and files maintained by the ISSC within each SSE. Records are inspected for compliance with this Order as well as other federal laws and guidelines applicable to IS. An IS Security Compliance Review addresses whether the system's technical security features are being bypassed or have vulnerabilities and whether procedures are being followed. Any security-relevant subject may be included by the ISSC for a compliance review. Issues such as the completion of security plans and contingency plans, employee awareness training, personnel background investigations, incident evaluation, operating system configurations, and access control procedures may be reviewed. The system owner shall use the results of the review to make improvements to the system's security.

902. REQUIREMENTS. The following inspection and report requirements will be followed by the ISS Division, the SSE and the system owner.

a. ISS Division. The ISS Division specialists shall conduct program reviews of each SSE's ISS program at least once every three years. A report of the program review will be completed within 30 days, marked at the appropriate level of sensitivity, and submitted to the ISS Division manager with a copy to the SSE. Report data will be compiled and used for evaluation, reference, statistics and future program reviews.

b. Headquarters, Regional and Center ISSC. SSE's ISSC shall conduct, at a least once every three years, IS security compliance reviews of locally certified information systems or IS components within their geographical area or national systems as assigned using the security plan package to evaluate the level of operational assurance for the systems. Any relevant security subject matter may be included by the ISSC for a compliance review.

(1) Reports. A report containing the results of each IS inspection will be marked at the appropriate level of sensitivity and forwarded to the ISS Division through the SSE division manager within 30 days of completion of the IS security compliance review. A copy may be forwarded to the regional line of business. The ISS Division will forward a copy to the ISSM at HQ for the affected line of business upon receipt of the approved report from the SSE. The ISS Division will maintain the report for evaluation, reference, statistics and future program reviews.

(2) Follow-up Reports. If follow-up action is required, a report will be submitted to the ISS Division containing action or non-action taken. A report will be submitted every 60 days until the affected issue(s) is closed out or until the ISS Division has determined that follow-ups may be deferred or discontinued.

c. System Owners. Upon notification by the ISSD or SSE, system owners shall perform self-inspections and monitoring in compliance with the system's security plan every three years or when an upgrade, major change or physical environment change occurs. The self-inspections will be kept locally, marked at the appropriate level of sensitivity, and will be made available for inspection to the ISSC or

special agents from the ISS Division upon request. Notification of completion of a self-inspection will be forwarded to the SSE and LOB ISSM.

903. SCHEDULES.

a. The ISS Division will develop a schedule of ISS program reviews at the end of each fiscal year for the following fiscal year.

b. The SSEs shall develop a schedule of security compliance reviews at the end of each fiscal year for the following fiscal year. A copy of the schedule, along with a summary of the results of the previous year's reviews, including system owner self-inspections, shall be forwarded to the ISS Division.

904 - 999. Reserved.

CHAPTER 10. SECURITY TEST AND EVALUATION

1000. SECURITY TEST AND EVALUATION (ST&E). This is the authorized, planned, systematic attempt to accomplish a system break-in. While ST&E is a very powerful technique for evaluating a system's security, it can cause serious disruptions to operations if prior coordination is not accomplished. ST&E Plan content will be addressed in guidelines from the ISS Division. In the FAA, there are three distinct types of ST&E.

a. SYSTEM SECURITY TESTING.

(1) Need. Security tends to degrade during the operational phase of the system life cycle. Organizations can use two basic methods to maintain operational assurance for a system:

(a) System inspection. An inspection can vary widely in scope: it may examine an entire system for the purpose of security assurance or it may investigate a single anomalous event. Inspections can be self-administered or independent, however they are conducted internally only. System inspection can provide excellent information about the technical, procedural, managerial, and other aspects of security.

(b) Monitoring. An ongoing activity that checks on the system for purposes of maintenance, ensuring system availability and integrity, protecting a system and its users from abusive or unlawful conduct, and protecting the rights or property of the provider of that service. ***However, all employees and contractors are advised that unauthorized or criminal activity discovered during the normal course of business will be reported to management, the SSE and, if necessary, appropriate law enforcement agencies for administrative, civil or criminal action.***

(2) Schedule. A schedule for self-inspections and system monitoring shall be built into the system's ISS plan and shall be accomplished as directed, once the system is fielded.

b. VULNERABILITY TESTING. This is the testing of an information system in a lab environment, test facility or any off-line area and is neither connected to any operational system nor will the testing in any way use the public switched system. It can be part of developmental or operational testing (DT&E/OT&E)of system requirements or an initial risk assessment. It is the FAA policy that no vulnerability testing will be conducted in, to or from any FAA facility, without the prior written notification to the DAA, ISS Division, and network administrators at the selected ST&E facility to eliminate the possibility of interference with other testing or operations that may be in progress. The notification shall include a ST&E Plan stating the parameters of the test (limits on actions that are allowed). An evaluation report stating all test results and subsequent action taken will be attached to the ST&E Plan and included in the Security Plan Package along with a copy of the test approval. Testing documents will be marked in accordance with Appendix 8 of this Order. OT&E test documents may be substituted for a ST&E plan as long as notifications are made and documented. Screening Information Requests (SIR) and contracts for leased goods or services should include appropriate consent clauses in accordance with Chapter 3 of this Order.

c. PENETRATION TESTING. This is testing of an information system that has been deployed for *operations* or is connected to an *operational* system or entrance to the system will require use of a public switched network (See definitions for "operations" and "operational") It is the FAA policy that no penetration testing will be conducted in, to or from any FAA facility without the prior approval of the DAA, system owner, and coordination with the ISS Division and the Office of the Chief Counsel (AGC). The request for approval shall include a ST&E Plan stating the parameters of the test (limits on actions that are allowed). Written permission from the DAA shall be the only authorization to conduct penetration testing of any FAA information system. A copy of the testing approval and an evaluation report of all test results and subsequent action taken will be attached to the ST&E Plan and included in the Security Plan Package. Testing documents will be marked in accordance with Appendix 8 of this Order.

1001. DISPOSAL OF TEST MEDIA. Copies of all documents, test results, instructions, reports and diskettes or other related material on media, will be given to the system owner or designee.

1002. UNAUTHORIZED TESTING. Conducting unauthorized testing or exceeding the parameters of the approved testing parameters could result in interference with U.S. Government information systems and is grounds for potential administrative, civil or criminal action. Unapproved testing could result in involvement of law enforcement in response to an incident, violation of Federal, state or local laws, or waste of valuable resources. Evidence of unauthorized testing will be collected in accordance with Paragraph 1109 of this Order and may be grounds for potential disciplinary action, or personal civil or criminal liability.

1003. ST&E PLAN. There are several legalities that must be taken into consideration before conducting either vulnerability or penetration testing and procedures for compliance must be included in the ST&E Plan for either type of testing.

a. Disclosure of communications. Individuals involved in testing will not disclose the contents of any data intercepted to other individuals for any purpose except as discussed below.

b. Notifications. For both vulnerability and penetration testing, there are required approvals as stated in paragraph 1000. However, in the case of penetration testing, because of Federal, state and local laws, there are additional notifications that must be made and copies of the notifications and approvals must be included in the ST&E plan.

(1) Because it is a violation of Federal law to use a public switched network (PSN) to penetrate a U.S. Government information system, notification must be made to the service provider of the PSN that will be used for the penetration testing. Greater assurances of consent may be required when a non-FAA provider is the target of any penetration test. Memoranda of Agreement may be negotiated with the PSN service providers to facilitate future notifications. Include copies of "consent clauses" from contracts providing or using goods or services not FAA owned. The PSNs that will be notified are those at the testing facility and at the facility where the system being tested is located.

(2) Notification to the responding law enforcement organizations (see paragraph 1101).

(3) Notification to the user community is appropriate when their consent has been previously obtained by other means..

c. Contraband. Contraband is any data that it is a violation of Federal, state or local law to possess no matter what form the data takes. If during testing, contraband data is accidentally discovered, the ISSD or the SSE will be notified. The appropriate law enforcement organizations (DOT Office of the Inspector General, FBI or other law enforcement agencies) will immediately be notified by ACS. All automated and manual documents, records, or automated media will be secured immediately until the arrival of law enforcement or until SSE or ISSD notification that the data is no longer needed.

1004 - 1099. RESERVED.

CHAPTER 11. SECURITY INCIDENTS: VIOLATIONS AND COMPROMISES

1100. GENERAL. An information system security incident is an event that has actual—or the potential for—adverse effects on computer or network operations. Such incidents can result in fraud, waste, or abuse; can compromise information; or can cause loss or damage to property or information. An incident can result from a computer virus, other malicious code, employee malfeasance, or a system intruder, either an insider or an outsider. Although it is known that hackers and malicious code can pose serious threats to systems and networks, actual incidents of such damage cannot be predicted. Security incidents, such as break-ins and service disruptions, on larger networks (e.g., the Internet), have harmed the computing capabilities or various organizations.

1101. REQUIREMENTS. All ISS incidents must be reported to the ISSD or ISSC within the SSE and to the system owner. All incidents shall be handled in accordance with procedures established in this Order. The SSE will be responsible for notifying the DOT Office of the Inspector General (DOT OIG), FBI, other appropriate law enforcement agencies as well as the Departmental Security Officer within the Office of the CIO. Except as noted below, DOT OIG will be notified of all ISS incidents.

1102. OBJECTIVE. The objective of the response procedures to security incidents shall be the swift detection of incidents and reaction and recovery as defined in the system's contingency plan or a contingency plan that includes system security incident response and recovery (See Chapter 2, Section 7, Contingency Planning).

1103. INFORMATION SYSTEM SECURITY INCIDENTS.

a. Intrusion. This is any deliberate attempt by any individual or group to gain unauthorized access or in excess of their authority to a system or interfere with the correct operation of any portion of any information system.

b. Malicious Code. This refers to viruses, worms, Trojan horses, logic bombs, and other uninvited software.

c. Fraud and Theft. Information systems can be exploited for fraud and theft both by automating traditional methods of fraud and by using new methods. Systems that control access to any resource are targets (e.g., time and attendance systems, financial systems, inventory systems, and long-distance telephone systems). Information system fraud and theft can be committed by insiders or outsiders. Insiders are responsible for most incidents of fraud.

d. **Employee Sabotage and Abuse.** Employees are most familiar with their employer's information systems and know which actions might cause the most damage, mischief, or sabotage. Common examples of information system-related sabotage include:

(1) Destroying hardware or facilities.

(2) Planting logic bombs that destroy programs or data.

(3) Entering data incorrectly.

(4) Crashing systems.

(5) Deleting data.

(6) Changing data.

The following incidents, while reportable to the ISSD and the ISSC within the SSE, need not be reported to the DOT OIG unless there is a pattern of incidents. The local law enforcement agency may be notified as appropriate.

e. Denial of service. The information system is not available for use to authorized personnel due to deliberate or accidental interference with system operations.

f. Computer viruses (report to DOT OIG if there is no eradication remedy in the virus detection software).

g. Errors and Omissions. Errors and omissions can be caused during the creation or modification of data.

h. Loss, Theft, or Damage. Computer equipment, software, and data may be misplaced, stolen, or physically damaged.

1104. DETECTION.

a. Intrusion Detection. This process identifies attempts to penetrate a system and gain unauthorized access or access in excess of authority. Real-time intrusion detection—examining audit records as they are created or using warning flags/notices—is primarily aimed at outsiders attempting to gain unauthorized access to the system. Examination of audit records may also be used to detect user errors and omissions and to detect fraud and abuse. Such examinations may also detect changes in the system's performance, which may indicate, for example, a virus or worm attack. There may be difficulties in implementing real-time auditing, including the degradation of system performance. However, intrusion detection provides two important functions in protecting information system assets:

(1) A feedback mechanism that informs the security staff about the effectiveness of other components of the security system. In this sense, intrusion detection is like a report card for perimeter defense subsystems such as firewalls and dial-up access control systems. The lack of detected intrusions is an indication that the perimeter defenses are working, if a robust and effective intrusion detection system is in place.

(2) A trigger or gating mechanism that determines when to activate planned responses to an incident.

b. After-the-Fact Identification. This process indicates that unauthorized access or access in excess of authority was attempted, successfully or unsuccessfully. Methods used may include reviewing audit logs, use of monitoring tools, integrity-monitoring tools, and software forensics. Attention can then be given to damage assessment, reporting requirements, investigation, and recovery operations.

1105. COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC). The purpose of the CSIRC is to protect FAA information systems from intrusions and other malicious activity and should any data or information system be compromised, to eradicate the problem and return the system operations as quickly as possible. The CSIRC Concept of Operations (limited distribution) is based on this order and establishes the procedures that will be implemented.

1106. INFORMATION SYSTEMS SECURITY NOTIFICATION MESSAGES. These numbered messages are distributed by the ISS Division at FAA Headquarters or the regional/center SSE. Distribution will be limited to affected organizations and will be indicated on the message. The messages are of two types.

a. Information System Security Alert Messages (ISS Alert). These messages contain information that must be acted on immediately. There will also be instructions for reporting action taken or negative replies to the ISS Division and cancellation date.

b. Information System Security Information Messages (ISS Info). These messages contain information of interest relating to IS security. There is no action required.

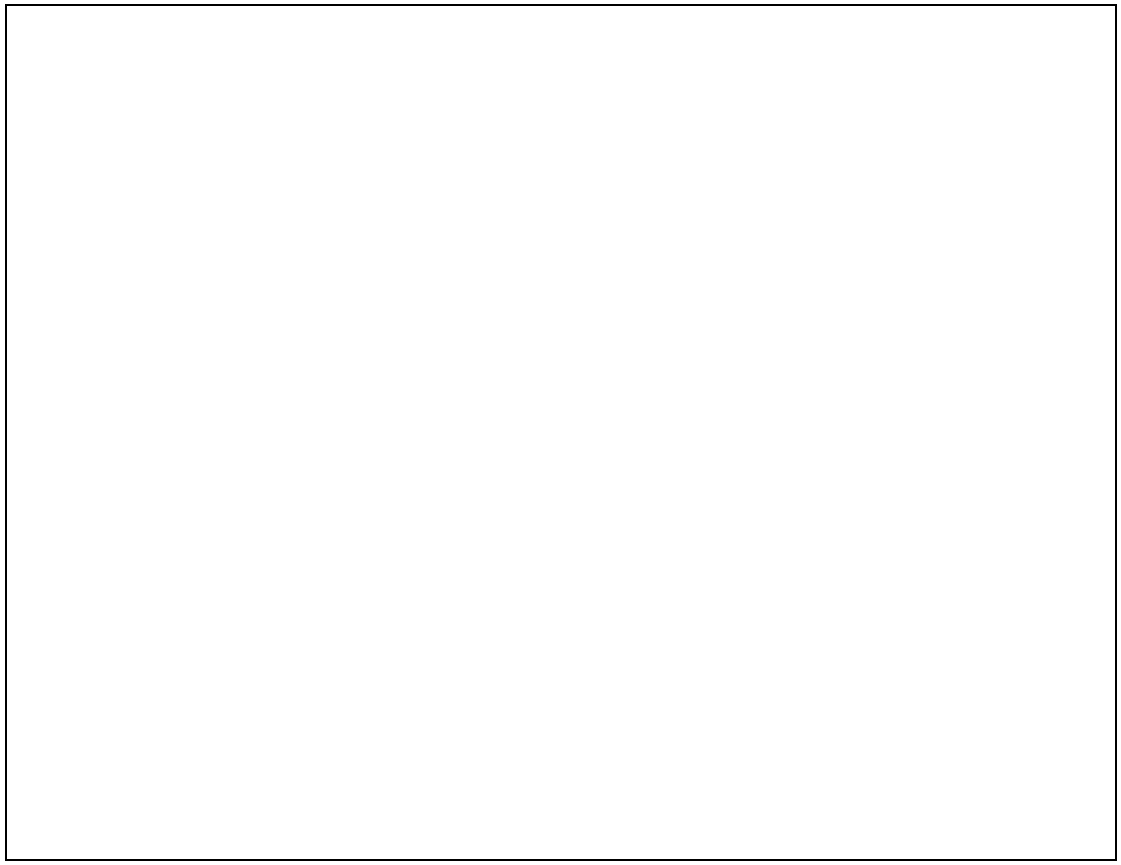
c. Numbering of ISS Alert and ISS Info messages. Numbering of these messages will be as follows.

(1) Headquarters originated. Messages from the ISS Division will begin with "ACO" plus the fiscal year and begin with 01 (Example: ACO-98-01). A capital letter will be attached to this series if there are subsequent messages relating to the topic of the original message.

(2) SSE originated. Messages from the SSE will be numbered as indicated in paragraph 1106c(1), except "ACO" will be replaced with the regional three letter code.

d. Logging messages. The originator will maintain a log of the ISS messages sent and received. The messages will be maintained until canceled by the originator. The logs will be made available during program reviews with ISS Division Special Agents.

e. Distribution and responses. Distribution and responses will be in accordance with Figure 11-1.



NOTE: *Notification of the ISSM or SSE does not preclude notification of any local management. See Table 1-1.

Figure 11-1. ISS Alert and Information Message Structure

1107. PLANNING.

a. An important consideration during development of the contingency plan is the policy for addressing emergency response to information system security incidents. The system owner should incorporate an incident reaction policy that emphasizes either of the following:

(1) Protection during an incident. If management determines that the site is sufficiently critical, it may choose an approach whose primary goal is to protect and preserve the site facilities and to provide normalcy for its users as quickly as possible. Attempts will be made to actively interfere with the intruder's processes, prevent further access, and begin immediate damage assessment and recovery. This process may involve shutting down the facilities, closing off access to the network, or other drastic measures. The drawback is that unless the intruder is identified directly, the intruder may come back into the site by a different path or may attack another site. Although using this strategy for emergency response does not preclude later prosecution of the culprits, it may be more difficult to obtain needed evidence later.

(2) Pursuit during an incident. This approach, favored by law enforcement agencies and prosecutors, adopts the opposite philosophy and goals. The primary goal is to allow intruders to continue their activities at the site until the site can identify the intruders. If the intruder is identified, prosecution is not the only outcome possible. If the culprit is an employee, contractor or a student, the organization may choose to take disciplinary action.

1108. IMPLEMENTATION OF INTRUSION DETECTION. The system owner shall be responsible to determine the appropriate level of intrusion detection to be implemented for an information system. The intrusion detection controls to be implemented must be documented in the ISS plan. The following are recommended intrusion detection levels for information systems at the low, medium, and high risk levels.

a. Low Risk System. Minimum intrusion detection methods to be implemented include enabling software logging processes and alarm and alert functions, reviewing audit logs daily, training users on anomaly reporting, and reviewing all trouble reports.

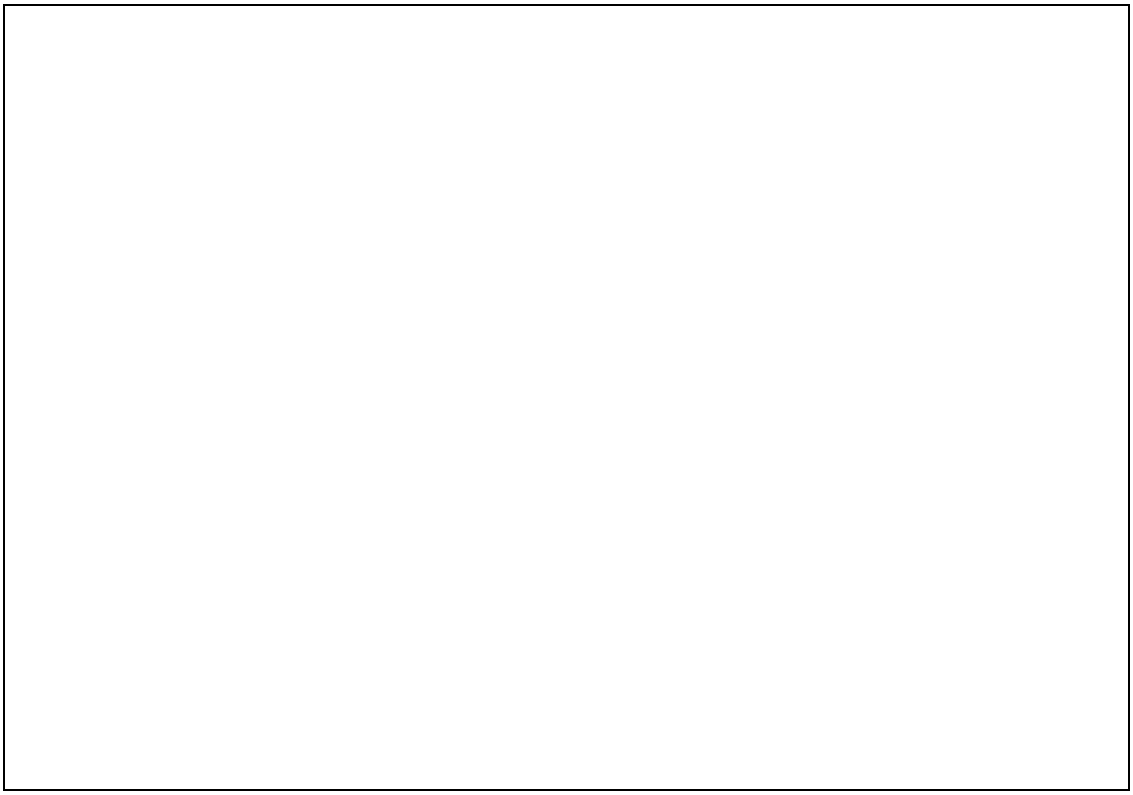
b. Medium Risk System. Minimum intrusion detection methods to be implemented include all controls listed for low risk systems, checking host based intrusion tools routinely, and establishing contact with the ISSC to obtain threat information.

c. High Risk System. Minimum intrusion detection methods to be implemented include all controls for medium risk systems. Critical servers shall also have redundant intrusion detection tools installed; and at logical network concentration points, intrusion detection tools, which monitor for traffic patterns consistent with known attacks, will be installed.

1109. REPORTING PROCEDURES.

a. Form. FAA-approved information system security incident reports shall be used for reporting and documenting incidents. See Appendix 3 for copies of the Information Systems Security Incident Report and the CERT[SM] Coordination Center Incident Report Form.

b. Notifications. Information system security incidents within a region or at a center shall be reported to the ISSC within the responsible SSE and the headquarters ISSM, who in turn will report to the DAA (See Figure 11-2). Incidents may be reported initially by telephone, followed by a submission of a completed Information Systems Security Incident Report form and the CERT[SM] Coordination Center Incident Report Form for Internet-based incidents. The ISSC shall report incidents to the ISS Division and shall provide ISS Division with a copy of the report marked with the sensitive security information (SSI) restrictive legend in Appendix 8 of this Order.



Legend: **Thin Line** **Block Line**
HQ Report Flow **Regional Report Flow**

NOTE: *Notification of the ISSM or SSE does not preclude notification of any local management. See Table 1-1.

Figure 11-2. ISS Incident Reporting Structure

(2) The following types of incidents shall be reported to the ISS Division or SSE:

(a) Unauthorized physical or logical access (internal and external) to FAA resources, such as, but not limited to the following items:

- Unauthorized physical or logical access to a local server or workstation
- Unauthorized physical or logical access to computer or network system devices (e.g., routers, hub, switch)
- Unauthorized access to equipment and cabling areas (e.g., LAN room, computer rooms, telephone closets, wire closets, wire troughs, equipment storage closets, etc.)
- Internet intrusion incidents (e.g. Denial of service attacks, unauthorized node discovery, unauthorized access to Intranet web sites, any other hacking attempts)
- All web server penetration, alterations, or damage
- All web-based attacks on user (e.g.., malicious Java applet)

(b) System abuse or misuse of Government systems, equipment, services, including but not limited to the following items:

- Use of computers, systems, services or materials for non-Government business (such as college course work), unless approved by the division manager.
- Use of computers, systems, or services for personal gain (including, but not limited to paid and non-paid consulting services, gambling, personal investments, etc.).
- Viewing, transmitting, possession of threatening, harassing, contraband in any format or media including but not limited to text, photographic, video, sound or other media. The content of which includes but is not limited to pornography, directions for making explosive or incendiary devices, hateful, threatening, or harassing content, and any other content which is prohibited by law.

(c) Fraud and Theft

- Theft of data
- Theft of software or source code
- All data protection violations (e.g. Privacy Act violation)
- Theft/damage of operational computer equipment
- Malicious code (e.g., viruses, Trojan horses)
- Denial of service, deliberate or accidental

(3) During incidents when compromise of the e-mail system is suspected, e-mail shall not be used for communicating about the response to an incident. Incidents discovered outside normal business hours shall be reported to the local FAA Operations Center, which will make the necessary notifications consistent with existing guidance.

(4) Incidents involving loss, theft, or damage to equipment must also be handled in accordance with FAA Order 4630.3, Survey of Lost, Damaged, or Destroyed Government Personal Property on a report of survey. In addition, a separate statement reporting the impact of loss of information will be sent to the SSE or ISSD and the ISSM on the approved FAA incident report form.

(5) Any inquiries by the media concerning an incident shall be forwarded to the FAA Public Affairs office.

1110. INVESTIGATIONS.

a. Investigations will be conducted by the SSE in accordance with FAA Order 1600.20, Civil Aviation Security Investigations Handbook. The ISSC should utilize the incident reporting procedures for allegations being investigated that meet the definition of an incident. See paragraph 1108 of this Chapter for incident reporting guidelines. The ISSC should emphasize during the investigation discovering the causes of incidents and ways to prevent further recurrences. Following are examples of incidents and the types of relevant investigations:

(1) In conjunction with, or in lieu of, an official investigation by the SSE of an event involving unauthorized disclosure or theft of sensitive electronic data, the ISSC shall submit a written report using the FAA-approved incident reporting form. The incident report will include a summary of the incident with all pertinent facts and a statement of corrective actions to prevent recurrence of the incident. See paragraph 1108 of this Chapter for reporting procedures.

(2) In conjunction with, or in lieu of, an official investigation by the SSE of an event involving unauthorized alteration or destruction of sensitive electronic data or software, the ISSC shall

submit a written report using the FAA-approved incident reporting form. The incident report will include a summary of the incident, including all pertinent facts, information on any disciplinary action taken by management, if available, and a statement of corrective action to prevent recurrence of the incident. See paragraph 1108 of this Chapter for reporting procedures.

(3) In the event of theft or sabotage of IS hardware, firmware, or software, the SSE shall be responsible for making the appropriate referrals and/or a determination regarding the conduct of an official investigation. The ISSC shall submit appropriate information to the ISS Division after obtaining approval from the investigating organization and the SSE. See paragraph 1108 of this Chapter for reporting procedures.

(4) In conjunction with, or in lieu of, an official investigation by the SSE of an event involving unauthorized access or access in excess of authority to an FAA information system or the misuse of information systems, the ISSC shall submit a written report using the FAA-approved incident reporting form. The incident report will include a summary of the incident with all pertinent facts, information on any disciplinary action taken by management, and a statement of corrective action to prevent recurrence of the incident. See paragraph 1108 of this Chapter for reporting procedures.

(5) When an incident occurs, it is FAA policy that the data, documents, logs, audit logs and other related data will be immediately secured and protected from unauthorized access and protected until such time as the SSE confirms that the data is no longer needed.

b. Requests for release of audit information and logs must be approved by the SSE.

c. Each ISSC will maintain a file of security incidents and a log of reported information about system security incidents. All documents shall be considered sensitive and safeguarded accordingly. The log will contain descriptive information regarding each information system security incident reported. The reports shall be reviewed and compared for trends that indicate areas in the security program that need strengthening.

1111. RECOVERY OPERATIONS. If system operations are affected by an incident, procedures identified in the contingency plan should be implemented. Any activity that could affect the preservation of evidence shall first be coordinated with the ISSC to ensure that investigations are not hindered. Any recovery action will be reported on the FAA-approved incident reporting form.

1112 - 1199. RESERVED.

CHAPTER 12. DECOMMISSIONING

1200. IS Decommissioning. Decommissioning of systems is considered a major system change and, therefore, requires a risk assessment. An ISS risk assessment will be conducted prior to decommissioning, and the safeguards will be included in the decommissioning plan as part of the security plan package. Any additional safeguards that are implemented during decommissioning, but are not included in the risk assessment, will be documented and attached to that assessment. There are two types of decommissioning:

(1) Decommissioning of systems with no replacement. This occurs when a system reaches the end of its useful life without being replaced. An ISS risk assessment includes all aspects of security to account for and protect the information, software, and hardware associated with the defunct system. Authentication and other interface data may remain in the software and on hard drives and could be a factor in supporting the need to destroy those parts of the software and hardware that are no longer reusable or needed. If hardware or software will be retained for reuse, then the data must be erased so as to be unreadable if retrieved. In some cases, software and pertinent data must be retained for legal or other purposes. Safeguards must then be implemented to secure the data and software from unauthorized access. These measures will be accounted for in the decommissioning risk assessment for the system. Copies of the finalized security plan package will be kept by the office that decommissioned the system and the ISS Division for one-year following decommissioning.

(2) Decommissioning of systems with transition to a new system. This occurs when tasks and information from a legacy system are transitioned to new technology. ISS risk assessments will include technical, physical, and personnel security. The risk assessment must address, but is not limited to, interfaces, time periods of concurrent operations, transfer of information between systems, new sites, sites not directly under FAA oversight, and any additional functions or data. Each presents vulnerabilities that may need special safeguards for a short time before transitioning to the permanent new generation environment. Transfer of sensitive operational data from a legacy system into a new or other existing system could change the level of security required to protect the data. If there is any doubt about the level of sensitivity of data or a system, ISS Division or the regional SSE can provide guidance. The ISS risk assessment will be included in the security plan package of the decommissioned system. A copy of the finalized security plan package will be kept by the office that decommissioned the system, the ISS Division, and the office that commissioned the new system.

1201. HARDCOPY RECORD DISPOSAL. Hardcopy records containing sensitive data shall be disposed of according to the following Orders:

a. FAA Order 1350.14, Record Management.

b. FAA Order 1350.15, Record Organization, Transfer and Destruction.

c. FAA Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information

d. FAA Order 1600.8, Communications Security (COMSEC) and Electronic Key Management Systems (EKMS)

1202. SOFTCOPY RECORD AND DATA DISPOSAL.

a. Records management shall indicate whether softcopy files containing the records involved have been destroyed according to the approved procedures described below. Data and records of security level CS2 (Chapter 2, section 2 and Table 2-4) or lower shall be destroyed by one of the following methods:

(1) Erasure with a degaussing device. Contact the ISSC or ISS Division for guidance on degaussing devices. After degaussing, floppy diskettes, tape, and other soft mylar media may be reused at any sensitivity level or may be disposed of as ordinary trash. (Harder-surface removable media

(e.g., Bernoulli disks) will be rendered unusable by the degaussing, because the intense magnetic fields used will warp the read and write heads.)

(1) Overwriting by a utility. The ISS Division can provide a list of utilities and procedures that are acceptable for disposing of any data. For example, removable soft media, including CD-RW, can be erased with three passes of writing random bit patterns over the entire media surface, followed by executing the media format routine.

(2) Shredding. Soft mylar-like media (e.g., diskettes, tape but excluding exterior casing) can be processed like paper through an approved shredder.

(3) CD-R. The material CD-Rs are made from are considered a solid waste by EPA and according to NIST are toxic when burned. Therefore, burning shall not be used as a disposal method. CD-Rs should be broken into at least 4 pieces and disposed of through an approved recycling program.

b. After erasure, media used on CS level 3 systems may be reused at the same security level by another application. Media for CS level 3 shall be erased thoroughly overwriting by an approved utility.

c. After being overwritten or degaussed as prescribed above, usable media may be recycled as follows:

(1) Provided that the media are used at the same sensitivity level or a more restrictive level, the media can be overwritten with new data without special procedural protections.

If no longer usable, contact the ISSD or SSE for instructions or disposal of equipment.

1203. DISPOSAL OF SURPLUS AND DEFECTIVE INFORMATION SYSTEM EQUIPMENT.

a. The information system storage media must be degaussed before disposal.

b. Information system equipment, used for processing or storing CS level 2 or less restrictive data, shall be erased using approved utilities. After this erasure, all visible markings indicating that the system was FAA owned shall be removed unless such removal will cause physical damage to the equipment. All visible markings showing that the equipment processed level CS3 sensitive data shall be removed.

c. Defective information systems can often be prepared for disposal by physically transferring storage media to an operational system and then erasing all records and data by using an approved utility for overwriting. If the medium is defective and cannot be erased, it shall be treated as though it contained classified data. For further guidance, see FAA Order 1600.2, chapter 12.

d. Reusable surplus information systems equipment shall be offered and advertised to other components within the FAA before the equipment is considered for disposal outside the FAA.

e. Surplus GOTS software shall be erased by using an approved utility for overwriting. The media shall then be treated at the security level of the GOTS software.

f. Surplus COTS software may be disposed of, provided that the owning organization can ensure that its reuse is authorized by software licenses and copyright constraints.

g. Surplus hardware can be shared with other Federal agencies; state governments; county, municipal, and local governments; and public schools. (Schools are authorized by P.L. 96-480, the Stevenson-Wydler Technology Innovation Act of 1980. The GSA can provide assistance with information system equipment disposal.)

h. Surplus software can be shared, in accordance with its licensing agreements, as in (f) above. Further information may be available from the Department of Energy, which has a pilot program for reusing and sharing COTS software.

i. Broken information system equipment must be disposed of in an environmentally sound manner. Workstations contain batteries, which must be removed before the workstations can be disposed of in a landfill. Broken circuit cards are classified as hazardous waste and cannot be put in a landfill

although unbroken circuit cards are considered benign. Broken monitors cannot be placed into trash intended for disposal in a landfill.

1204 - 1299. RESERVED.

APPENDIX 1. ACRONYMS AND DEFINITION OF TERMS

APPENDIX 1. ACRONYMS AND DEFINITION OF TERMS

1.1 ACRONYMS

ADP	automated data processing
ADTN	agency data telecommunications network
AIS	automated information systems
AMS	Acquisition Management System
ANSI	American National Standards Institute
AR	acquisition review
CA	Certifying Authority
CAS	Civil Aviation Security
CC	Common Criteria
CD	compact disk
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CM	configuration management
CS	commercial security
COMSEC	Communications Security
COTS	commercial off-the-shelf
CRDA	Cooperative Research and Development Act
DAA	Designated Approving Authority
DES	Data Encryption Standard
DIRMM	Departmental Information Resources Management Manual
DOD	Department of Defense
DOJ	Department of Justice
DOT	Department of Transportation
DSS	Digital Signature Standard
DTE	data terminal equipment
E-Mail	electronic mail
EIS	Enforcement Information System
EPL	evaluated products list
FAA	Federal Aviation Administration
FACA	Federal Advisory Committee Act
FAPM	Federal Aviation Personnel Manual
FAX	facsimile

FED-STD	Federal Telecommunications Standard
FIPS	Federal Information Processing Standards
FIRMR	Federal Information Resources Management Regulation
FMFIA	Federal Managers' Financial Integrity Act
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPM	Federal Personnel Manual
FPMR	Federal Property Management Regulations
GOTS	Government off-the-shelf
GSA	General Services Administration
HQ	headquarters
HTTP	hypertext transfer protocol
ID	identifier
IDS	intrusion detection system
IETF	Internet Engineering Task Force
IPPS	Integrated Payroll and Personnel System
IPSEC	Internet Protocol Security
IPT	Integrated Product Team
IRM	Information Resource Management
IS	information system
ISO	International Standards Organization
ISS	information systems security
ISSC	information systems security coordinator
ISSD	Information Systems Security Division
ISSM	information systems security manager
ISSO	information systems security officer
ISSP	Information Systems Security Program
IT	information technology
JRC	Joint Resources Council
LAN	Local Area Network
LOB	line of business
MAN	metropolitan area network
MNS	mission need statement
MOA	memorandum of agreement
MOU	memorandum of understanding

NACI	National Agency Check and Inquiry
NAS	National Airspace System
NBID	network-based intrusion detection
NDI	nondevelopment item
NII	National Information Infrastructure
NIMS	NAS Infrastructure Management System
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PA	process area
PBX	Private Branch Exchanges
PC	personal computer
PCCIP	Presidential Commission of Critical Infrastructure Protection
PDD	Presidential Decision Directive
PL	Public Law
PSN	public switched network
PUB	publication
RBAC	Role-based access control
RFC	Request for Comments
RSA	Rivest, Shamir and Adelman
SES	Senior Executive Service
SHS	Secure Hash Standard
SIR	Screening Information Request
SMTP	simple mail transfer protocol
SOW	Statement of Work
SPL	security performance level
SSE	servicing security element
SSE-CMM	System Security Engineering Capability Maturity Model
SSI	sensitive security information
ST&E	security test and evaluation
S/WAN	secure/WAN
TBD	to be determined
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
VPN	Virtual Private Network

WAIS	Wide Area Information Service
WAAS	Wide Area Augmentation System
WAN	Wide Area Network
WWW	World Wide Web

1.2 DEFINITION OF TERMS

Acceptable risk. Risk that is acceptable to a Designated Approving Authority (DAA) because of the cost and magnitude of implementing security countermeasures.

Accountability. The quality or state which enables violations or attempted violations of information system security to be traced to individuals who may then be held responsible.

Acquisition/development/installation/implementation controls. The process of ensuring that adequate security controls are considered, evaluated, selected, designed, and built into the system during its early planning and development stages and that an ongoing process is established to ensure continued operation at an acceptable level of risk during the installation, implementation, and operation stages.

Adequate protection. Protection that is commensurate with the risk and magnitude of the potential harm resulting from the loss, misuse, or unauthorized access to or modification of information resources. This protection includes ensuring that systems and applications used by the FAA operate effectively and provide appropriate confidentiality, integrity, availability, and accountability by using cost-effective management, personnel, operational, physical, and technical controls.

Application. A computer program or similar set of instructions or codes that directs the operation of an information system to perform a specified function or operation. Applications are information resources used to satisfy a specific set of user requirements.

Authentication. A measure designed to provide protection against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator.

Authorization. A written decision by the Designated Approving Authority (DAA) to permit a major application or general support system to process FAA information in the performance of the FAA mission in an operational environment. Authorization is based, in part, on ISS certification. For systems that process FAA information, processing shall be reauthorized at least every 3 years. The DAA may issue interim authorization from ISS requirements and security plans, thereby accepting the increased associated risk until named requirements are met.

Authorize processing. The management authorization to operate a system; this authorization is based on an assessment of management, operational, and technical controls. By authorizing processing in a system, the DAA accepts the risk associated with it.

Availability. The accessibility to information or a system on a timely basis to support mission requirements and deadlines. An important measure of availability (i.e., the criticality) is the length of time that the system can be nonoperational without affecting the organization's mission. For example, a payroll system cannot be down for weeks because employees expect to be paid on time. Contingency plans, disaster recovery plans, redundancy, and systems and information backups are security practices that contribute to availability.

Center. In this Order, refers to the Mike Monroney Aeronautical Center and the William J. Hughes Technical Center. This term is usually used in conjunction with the term "region".

Certification. Review by the Certifying Authority (CA) to determine whether a system meets applicable federal standards and policies and that the security plan contains those requirements.

Certifying Authority (CA). A manager that certifies a system's security based on required documentation. The CA for ACS is the ISS Division Manager, who may designate other CAs in writing for a single system or multiple systems.

Commercial Security (CS) Levels. This term is used to describe the security levels for categorized information based on NIST document, *Common Criteria for Information Technology*, and the International Standards Organization document, *ISO/IEC Guide for Production of PP and ST, Version 0.6, #JTC 1/SC27/WG3N452.*

Confidentiality. A requirement that private or confidential information not be disclosed to unauthorized individuals.

Contraband. Contraband is any data that it is a violation of Federal, state or local law to possess no matter what form the data takes. An example of contraband is child pornography.

Designated approving authority (DAA). A senior FAA management official with decision-making and fiscal responsibilities for information systems within their authority. The DAA formally assumes responsibility for allocating resources to achieve an acceptable level of security, remedy security deficiencies, and authorize operation of an information system at an acceptable level of risk (i.e., adequate protection).

Developer or developing organization. For purposes of this Order, these terms refer to the FAA developer or developing organization. If a system is contracted out, the vendor carries out the task of development, however, the ISS responsibilities encompassing development resides with the FAA.

FAA facility. Any facility that is owned, leased or lent to the FAA where FAA information systems, or any portion of FAA information systems, will be developed, housed or operated. It is not necessary that the equipment be owned by the U.S. Government, only operated for the U.S. Government in accordance with the National Information Infrastructure Act of 1996.

General support system. An interconnected set of information resources that share a common functionality under the same direct management control. These systems, which include software, host computers (mainframes, minis, workstations) and networks (LANs and WANs), provide support for a variety of users and applications. Even if none of the individual applications is sensitive, the support system may be considered sensitive, if overall, the aggregate of applications and support provided are critical to the mission of the agency.

Government facility. For purposes of this Order, any facility that is owned by Federal, state, county, municipal, tribal or foreign governments.

Government information. Information that is created, collected, processed, disseminated, or disposed of by or for the Federal Government.

Information. Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms. FAA information is categorized into one of three groups:

a. Classified information. Information that, in the interest of national security, requires protection against unauthorized disclosure. Such information is classified top secret, secret, or confidential. Classified information is beyond the scope of this Order.

b. Sensitive information. Information whose unauthorized disclosure, modification, or unavailability would harm the agency Sensitive information includes:

(1) Essential or critical air traffic control data and any other information that must be protected in performance of an FAA mission to ensure confidentiality, integrity, or availability of information

(2) Information identified in Executive Order 12958, requiring protection under the provisions of the Privacy Act of 1974

(3) Information designated “For Official Use Only” (FOUO)

(4) Information whose disclosure or modification might impact on the contractual or resource management function

(5) Proprietary information

(6) Information identified in the Information Technology Management Reform Act of 1996

(7) Information falling under the auspices of the Computer Security Act of 1987

(8) Information protected under the Sensitive Security Information rule 14 CFR , Part 191, et al.

(9) Financial management information

(10) Information exempt from disclosure under the Freedom of Information Act (FOIA)

c. Nonsensitive information. Information that is neither classified nor sensitive and, therefore, does not warrant protective marking, handling or disposition.

Information assurance. Policies and procedures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This assurance includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information life cycle. The stages through which information passes typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

Information owner. The owner of information that originates in the FAA is the manager responsible for establishing the rules appropriate for the use and protection of the subject data/information. For information originating elsewhere, the information owner is the originating entity, represented by a designated individual. The information owner retains responsibility and authority even when the data/information are shared with other organizations.

Information resources. Both government information and information technology resources. These include computer or communications systems, transmission facilities or networks, or combinations of these.

Information resources management. The process of managing information resources to accomplish agency missions. This term encompasses both the information and the related resources, such as personnel, equipment, funds, and information technology.

Information system. A discrete set of information resources either in stand-alone or networked configurations, that is organized for the collection, processing, maintenance, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Information systems are of two types:

a. General support systems. Interconnected information resources that are under the same direct management control and share common functionality.

b. Major application systems. Systems that require special management attention because of their importance to the agency's mission; their high-maintenance, development, or operating costs; or their significant role in dealing with the agency's programs, finances, property, or other resources.

Information system life cycle. The phases through which an information system passes typically characterized as initiation, development, operation, and termination.

Information systems security (ISS). The collected attributes that describe the security aspects of FAA information resources, either individually or collectively.

Information technology. The hardware, software, and networks that process information, regardless of the technology involved, whether computers, telecommunications, or others. **Integrity.** Data integrity is a requirement that information and programs are changed only in a specified and authorized manner. System integrity is a requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

ISS certification. Certification that an information system meets applicable federal standards and the requirements contained in the system's ISS plan.

ISS plan. A document that identifies the information system components; operational environment; sensitivity and risks; and detailed, cost-effective measures to protect the system. The ISS plan must be maintained throughout the system life cycle and is complete when selected controls are tested and the plan is signed by the responsible FAA official.

ISS program (ISSP). All programs, policies, and procedures to protect sensitive FAA information and information systems.

Line of Business (LOB). For purposes of this Order, LOB means an organization or group of organizations that reports directly to the Administrator (e.g., Assistant Administrator for Regional and Center Operations) or a group of organizations that report to an Associate Administrator.

Major application. An application that requires special attention to security because of the risk and magnitude of the harm that could result from the loss, misuse, or unauthorized access to, or modification of, the information in the application. Such a system might actually comprise many individual application programs and hardware, software, and

telecommunications components. To be classed as a major application for security purposes, the confidentiality, integrity, or availability of the system must be rated medium or high. Systems designated as "major information systems" shall be considered major applications for security purposes.

Networks. Communications hardware and software that allow one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area networks (LANs), or wide area networks (WANs), and public networks such as the Internet.

Non-FAA facility. Any facility that is not owned or leased by the FAA where FAA information systems, or any portion of FAA information systems, will be developed, housed or operated. It is not necessary that the equipment be owned by the U.S. Government, only operated for the U.S. Government in accordance with the National Information Infrastructure Act of 1996.

Non-government facility. For purposes of this Order, any facility that is not owned by Federal, state, county, municipal, tribal or foreign governments.

Operational controls or operations. The day-to-day procedures and mechanisms used to protect operational systems and applications. Operational controls affect the system and application environment. For purposes of this Order, this term applies to any LOB's operations, not just the NAS.

Penetration testing. This is testing of an information system that has been deployed for *operations* or is connected to an *operational* system or entrance to the system will require use of a public switched network.

Personnel security. This program provides a basis for security determinations for sensitive positions, clearances for access to classified material, and suitability for Federal employment. The program is concerned not only with an individual's suitability and loyalty to the United States, but also with questionable habits, character, and associations and personal reliability, judgment, and susceptibility to coercion. All issues are to be resolved as favorable if the access to sensitive information is determined to be clearly in the interest of National Security. The authority for this program is the same as that for the investigations program. Internal guidance is provided by Order 1600.1, Personnel Security Program.

Physical security. The combination of security controls that bar, detect, monitor, restrict, or otherwise control access to sensitive areas. Physical security also refers to the measures for protecting a facility that houses ISS assets and its contents from damage by accident, malicious intent, fire, loss of utilities, environmental hazards, and unauthorized access.

Product. A package of information technology (IT) software and/or hardware, providing functionality designed for use or incorporation within a multiplicity of systems.

Protection profile (PP). A combination of security requirements, including assurance and functional requirements, with the associated rationale and target environment to meet identified security needs.

Residual risk. The remaining risk as a result of assessing existing security controls and mitigating vulnerabilities through risk management.

Risk. Identifiable threats (e.g., disclosure, modification, or loss of data) that have some probability of occurring and causing loss or damage to a system. See also risk analysis and risk management below.

Risk analysis. A structured approach to identifying assets, determining threats and vulnerabilities, and identifying cost-effective controls to protect the system. The two general categories of risk analyses are quantitative (estimating risks in terms of dollar losses) and qualitative (empirical estimates of risk, e.g., high, medium, low).

Risk management. The policies and procedures for identifying risks and reducing them to an acceptable level by applying cost-effective safeguards (e.g., passwords, backup). In the FAA, risk assessments encompass risk management concepts and the two terms are sometimes used synonymously.

Safeguards. The protective measures for a system. System security measures and countermeasures, safeguards, and controls are used interchangeably in this order.

Security specification. A detailed description of the safeguards required to protect a sensitive application.

Security level. An indication of the seriousness of the impact or loss to the FAA in case of an unauthorized inaccuracy, alteration, disclosure, or unavailability of information. Security levels are hierarchically arranged with 1 indicating the least impact and 3 indicating the most impact. A security level may be applied to information, applications (i.e., computer programs), or information systems.

Sensitive information. Any information whose loss, misuse, unauthorized accessibility, or modification could adversely affect the national interest, the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act of 1974.

Servicing security element. The local security organization that provides security support for the ISS Program. In FAA headquarters, this is the Office of Civil Aviation Security Operations (ACO). In the regions and centers, these are the Civil Aviation Security Divisions (-700s and ACT-8).

System. A generic term that means either a major application or a general support system. IT products assembled together—either directly or with additional computer hardware, software, and/or firmware—and configured to perform a particular function within a particular operational environment.

System owner. The system owner is the manager responsible for the organization that operates the information system. In general, the system owner is responsible for setting policy and direction, but is NOT responsible for day-to-day operation. The information owner for information within, processed by, or transmitted by a system may or may not be the same as the system owner. Also, a single system may use information from multiple information owners.

System security plan. The OMB-formatted document that identifies the system components; sensitivity and risks; and the detailed, cost-effective safeguards to protect the system. The system security plan constitutes a qualitative risk analysis when the entire plan is completed, selected controls are tested, and the plan is signed.

Security testing and evaluation (ST&E). This is the authorized, planned, systematic attempt to accomplish a system break-in for purposes of evaluation of a system's security.

Threat. An activity, deliberate or unintentional, with the potential for causing harm to an information system or activity.

Vulnerability. A flaw or weakness that may allow harm to occur to an information system.

Vulnerability testing. This is the testing of an information system in a lab environment, test facility or any off-line area and is neither connected to any operational system nor will the testing in any way use the public switch system. It is part of operational testing of system requirements or an initial risk assessment.

APPENDIX 2. REFERENCES

APPENDIX 2. REFERENCES

LEGISLATION

1. Computer Security Act of 1987 (P.L. 100-235, codified as 18 USC 1030)
2. The Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 (amends 18 USC 1030)
3. National Information Infrastructure Act of 1996 (amends 18 USC, Section 1030)
4. Privacy Act (P.L. 93-579) of 1974
5. Electronic Communications Privacy Act (P.L. 99-508)
6. Computer Fraud and Abuse Act; Counterfeit Access Device Act (P.L. 99-474; P.L. 98-473)
7. Federal Managers Financial Integrity Act (P.L. 97-225)
8. Trade Secrets Act (18 U.S. Code)
9. Copyright Act of 1980 (17 U.S. Code)
10. Paperwork Reduction Act of 1980 & 1986 (P.L. 96-511/P.L. 99-500)
11. Computer Matching and Privacy Protection Act (P.L. 100-503)
12. Federal Property and Administrative Services Act of 1949
13. Clinger-Cohen Act, U.S. Code 1401 et seq.
14. Stevenson-Wydler Technology Innovation Act of 1980
15. Information Technology Act of 1996
17. 5 U.S. Code, Section 552
18. 49 U.S. Code, Section 40119
19. 17 U.S. Code, Section 106 and 504

EXECUTIVE ORDERS

1. Executive Order 13010, Critical Infrastructure Protection, July 15, 1996
2. Executive Order 13011, Federal Information Technology, July 16, 1996
3. Presidential Decision Directive #63, Critical Infrastructure Protection, May 1998
4. Executive Order 12958

FAA ORDERS

1. Order 1280.1, Protecting Privacy of Information About Individuals
2. Order 1350.14, Record Management
3. Order 1350.15, Record Organization, Transfer, and Destruction
4. Order 1370.79, Internet Policy
5. Order 1600.20, Civil Aviation Security Investigations Handbook
6. Order 1600.1, Personnel Security Program
7. Order 1600.2, Safeguarding Controls and Procedures for Classified National Security Information and Sensitive Unclassified Information, August 29, 1997
8. Order 1600.6, Physical Security Management Program

9. Order 1600.8, Communications Security (COMSEC)

10. Order 1600.54, FAA Automated Information Systems Security Handbook

11. Order 1900.47, Air Traffic Services Contingency Plan

12. Order 1800.8, National Air Systems Configuration Management

13. Order 1810.1 The FAA Acquisition Management System

14. Order 4630.3, Survey of Lost, Damaged, or Destroyed Government Personal Property

15. Federal Aviation Personnel Manual (FAPM) 2635, Conduct and Discipline

OMB CIRCULARS AND BULLETINS

1. OMB Circular A-130, Appendix III, Security of Federal Automated Information Systems, February 8, 1996

2. OMB Circular A-123 Revised, Internal Control Systems, June 21, 1995

3. OMB Circular A-127, Financial Management Systems, July 23, 1993

4. OMB Bulletin 90-08, Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information, July 9, 1990

OFFICE OF PERSONNEL (OPM) MANUALS AND REGULATIONS

1. 5 CFR Part 930, Training Requirements for the Computer Security Act

2. 5 CFR Part 930, Subpart C--Employees Responsible for the Management or Use of Federal Computer Systems, January 1992

3. 14 CFR, Part 191, Sensitive Security Information

4. 14 CFR, Part 201, Security and Privacy

5. Federal Personnel Manual, Chapter 731, Personnel Suitability, September 29, 1988

GENERAL SERVICES ADMINISTRATION (GSA) REGULATIONS AND BULLETINS

1. Federal Information Resources Management Regulation (FIRMR), Subpart 201-21.3, Security and Privacy, October 1990

2. Federal Information Resources Management Regulation (FIRMR), Part 201-39, 1001-1

3. Federal Information Resources Management Regulation (FIRMR), Part 201-23, Disposition

4. FIRMR Bulletin C-19, Information System Security (INFOSEC), January 30, 1991

5. FIRMR Bulletin C-28, Computer Viruses, November 6, 1991

6. FIRMR Bulletin C-2, Disposition and Reuse of Federal information Processing Equipment,

7. Federal Property Management Regulations (FPMR), Subchapter H, Part 101-43, Utilization of Personal Property, Part 101-44, Donation of Personal Property, Part 101-45, Sale, Abandonment, or Destruction of Personal Property, and Part 101-46, Utilization and Disposal of Personal Property Pursuant to Exchange/Sale Authority.

NIST: FEDERAL INFORMATION PROCESSING STANDARDS (FIPS)

1. FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management

2. FIPS PUB 41, Computer Security Guidelines for Implementing the Privacy Act of 1974

3. FIPS PUB 46-2, Data Encryption Standard (DES)

4. FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personnel Identification

5. FIPS PUB 65, Guideline for Automatic Data Processing Risk Analysis
6. FIPS PUB 73, Guidelines for Security of Computer Applications
7. FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard
8. FIPS PUB 81, DES Modes of Operation
9. FIPS PUB 83, Guideline on User Authentication Techniques for Computer Network Access Control
10. FIPS PUB 87, Guidelines for ADP Contingency Planning
11. FIPS PUB 88, Guideline on Integrity Assurance and Control in Database Administration
12. FIPS PUB 102, Guideline for Computer Security Certification and Accreditation
13. FIPS PUB 112, Standard on Password Usage
14. FIPS PUB 113, Standard on Computer Data Authentication
15. FIPS Publication 139, Interoperability and Security Requirements for Use of the Data Encryption Standard in the Physical Layer of Data Communications
16. FIPS PUB 140-1, Security Requirements for Cryptographic Modules
17. FIPS PUB 171, Key Management Using ANSI X.9.17
18. FIPS PUB 180-1, Secure Hash Standards (SHS)
19. FIPS PUB 181, Automated Password Generator
20. FIPS PUB 185, Escrowed Encryption Standard (EES)
21. FIPS PUB 186, Digital Signature Standard (DSS)
22. FIPS Publication 188, Standard Security Label for Information Transfer
23. FIPS Publication 190, Guideline for the Use of Advanced Authentication Technology Alternatives
24. FIPS Publication 191, Guideline for the Analysis of Local Area Network Security

NIST: SPECIAL PUBLICATIONS (SP) AND OTHER REPORTS

1. SP 500-74, Guide for Selecting Automated Risk Analysis Tools, October 1989
2. SP 500-120, Security of Personal Computer Systems: A Management Guide, January 1985
3. SP 500-133, Technology Assessment: Methods for Measuring the Level of Computer Security
4. SP 500-134, Guide on Selecting ADP Backup Process Alternatives
5. SP 500-137, Security for Dial-Up Lines
6. SP 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach
7. SP 500-156, Message Authentication Code (MAC) Validation System: Requirements and Procedures
8. SP 500-157, Smart Card Technology: New Methods for Computer Access Control
9. SP 500-160, Report of the Invitational Workshop on Integrity Policy in Computer Information Systems
10. SP PUB 500-166, Computer Viruses and Related Threats: A Management Guide
11. SP 500-169, Executive Guide to the Protection of Information Resources
12. SP 500-170, Management Guide to the Protection of Information
13. SP 500-171, Computer User's Guide to the Protection of Information Resources

14. SP 500-172, Computer Security Training Guidelines

15. SP 500-173, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach

16. SP 800-2, Public-Key Cryptography

17. SP 800-3, Establishing a Computer Security Incident Response Capability (CSIRC)

18. SP 800-4, Computer Security Considerations in Federal Procurements, A Guide for Procurement Initiators, Contracting Officers, and Computer Security Officials

19. SP 800-5, A Guide to the Selection of Anti-Virus Tools and Techniques

20. SP 800-6, Automated Tools for Testing Computer System Vulnerability

21. SP 800-7, Security In Open Systems

22. SP 800-9, Good Security Practices for Electronic Commerce, Including Electronic Data Interchange

23. SP 800-10, Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls

24. SP 800-12, An Introduction to Computer Security: The NIST Handbook

25. SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems

26. SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model

27. NISTIR 4659, Glossary of Computer Security Terminology

28. NISTIR 4667, Computer Security Bulletin Board System User's Guide

29. NISTIR 4749, Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out

30. NISTIR 4939, Threat Assessment of Malicious Code and External Attacks

31. NIST NCSL Bulletin, Data Encryption Standard

32. NIST (Final Draft), Common Criteria for Information Technology, August 14, 1998

DEPARTMENT OF TRANSPORTATION PUBLICATIONS

1. Departmental Information Resources Management Manual, (DIRMM), Chapter 11, Information Systems Security Policy, (DOT H 1350.2)

DOT Information Systems Security Directing Guidance

2. DOT Information Systems Security Guide (DOT H 1350.250)

3. DOT Network Security Guide (DOT H 1350.251)

4. DOT Information Systems Security Implementing Guidance

5. DOT Sensitive Systems Security Plans and Samples (DOT H 1350.260)

6. DOT Mainframe Environmental Security Software Standards (DOT H 1350.261) (Draft)

7. Office Automation Information Systems (OAIS) Security Handbook (DOT H 1350.262)

8. Model Continuity of Operations Plan (COOP) Guide (DOT H 1350.263)

9. Model Disaster Recovery Plan (DRP) for Local Area Networks and Automated Information Systems Guide (DOT H 1350.264)

10. Guide for Local Area Network (LAN)/Wide Area Network (WAN) Security (DOT H 1350.266)

11. DOT Guide for New Information Systems Security Officers: How To Establish An Information Systems Security Program (DOT H 1350.270)

12. Computer Incident Response Capability (DOT H 1350.271)

13. Guide for Department of Transportation Computer Security Training and Orientation Program (DOT H 1350.277)

14. Computer Security Guide for Senior Executives

15. Management Guide to the Protection of Information Resources

16. Information Systems Security: A Primer for Employee Awareness Orientation

OTHER GOVERNMENT PUBLICATIONS

1. Model Framework for Management Control Over Automated Information Systems, President's Council on Management Improvement and the President's Council on Integrity and Efficiency, January 1988

2. Information Technology Installation Security, Federal Systems Integration and Management Center (FEDSIM), GSA, December 1988

3. DOD 5200.28-Std Trusted Computer System Evaluation Criteria (TCSEC)

4. Department of Commerce Guidelines for Developing and Evaluating Security Plans for Sensitive and Classified Systems

NONGOVERNMENT PUBLICATIONS

1. Internet Engineering Task Force (IETF) Request for Comments (RFC) 1825-1829

2. System Security Engineering Capability Maturity Model (SSE-CMM)

APPENDIX 3. SAMPLE FORMS

APPENDIX 3. SAMPLE FORMS

Memorandum

U.S. Department
of Transportation

**Federal Aviation
Administration**

Subject: Sample Request for Approval to Use Personally Owned Computer Equipment or Software for Processing FAA-owned Data

Date:

From: Employee Name, Routing Symbol

Reply to
Attn of:

To: Manager, Routing Symbol

I request approval to use my personally owned computer and/or software to access and/or process Government data. I understand that all information created is the property of the U.S. Government. The records I will access or create off-site will be backed up daily and the backup media will stored in an FAA office. All data and records created will continue to be readable in the absence of my computer and/or software.

Sensitive data will be processed only with the restrictions specified below. By processing sensitive data, I personally assume responsibility for ensuring that integrity, confidentiality and availability of the data is maintained.

I understand and will comply with FAA Orders 1600.68, “Information Systems Security Policy and Responsibilities,” and 1600.69, “Information Systems Security Program,” and 1350.22A, “Protecting Privacy of Information About Individuals”.

<Gov't employee>I understand that, according to the Fair Labor Standards Act, I am exempt and will not be compensated for my time spent on work approved by this agreement unless this request is part of an approved telecommuting agreement.

OR

<Contractor>I understand that, under the requirements of the contract my employer has with the FAA, that I may not be compensated by the FAA for my time spent on work approved by this agreement.

I understand that the FAA does not assume any responsibility for the safety, maintenance, security, or operation of the equipment, and the hardware, software and data are subject to inspection. Failure to permit an inspection as requested by the FAA will be cause for immediate termination of this agreement.

I understand that I must implement access control, such as password protection, for my system and prohibit access to FAA-owned sensitive data by other individuals.

I understand that I must comply with the copyright laws that pertain to any software borrowed from the FAA or used on FAA computers.

I understand that I am required to install FAA-licensed virus-checking software, to maintain the current release, and to use the software at all times on my system.

Identification of Data to be Accessed: _____

Identification of Data to be Taken Off-site: _____

Government-licensed Software to be Issued: _____

Personally-owned Software to be Installed: _____

Serial number of Personally-owned Software: _____

Virus-checking Software to be Issued: _____

FAA Location for Storage of Backups: _____

Identification of FAA Computer to be Accessed Remotely: _____

Employee Name: _____

Location of Personally Owned Computer: _____

Serial Number of Personally Owned Computer: _____

Contract Number: _____

Contract Company Name: _____

Expiration Date of This Agreement: _____

FAA-Mandated Protections for Sensitive Data: _____

_____

_____

_____

_____ _____

Signature, Requesting Employee Date of Request

[ ] Approved

[ ] Disapproved

_____ _____

Signature, Approving FAA Official Date of Approval

version 3.0
February 28, 1996

CERT(sm) Coordination Center
Incident Reporting Form

The CERT Coordination Center (CERT/CC) has developed the following form in an effort to gather incident information. We would appreciate your completing the form below in as much detail as possible. The information is optional, but from our experience we have found that having the answers to all the questions enables us to provide the best assistance. Completing the form also helps avoid delays while we get back to you requesting the information we need in order to help you. Sites have told us, as well, that filling out the form has helped them work through the incident.

Note that our policy is to keep any information specific to your site confidential unless we receive your permission to release that information.

Please feel free to duplicate any section as required. Please return this form to cert@cert.org. If you are unable to email this form, please send it by FAX. The CERT/CC FAX number is

+1 412 268 6989

Thank you for your cooperation and help.
.....

1.0. General Information

1.1. Incident number (to be assigned by the CERT/CC): CERT#

1.2. Reporting site information

1.2.1. Name (e.g., CERT Coordination Center):

1.2.2. Domain Name (e.g., cert.org):

1.2.3. Brief description of the organization:

1.2.4. Is your site an Internet Service Provider (Yes/No):

2.0. Contact Information

2.1. Your contact information

2.1.1. Name:
2.1.2. Email address:
2.1.3. Telephone number:
2.1.4. FAX number:
2.1.5. Pager number:
2.1.6. Home telephone number (for CERT/CC internal use only):

2.1.7. Secure communication channel (e.g., PGP, PEM, DES, secure telephone/FAX) [NOTE -- we will call to obtain the secure communication channel information] (Yes/No):

2.2. Additional contact information (if available)

2.2.1. Name:
2.2.2. Email address:
2.2.3. Telephone number:
2.2.4. FAX number:
2.2.5. Pager number:
2.2.6. Home telephone number (for CERT/CC internal use only):
2.2.7. Secure communication channel (Yes/No):

2.3. Site security contact information (if applicable)

2.3.1. Name: see 2.1 above
2.3.2. Email address:
2.3.3. Telephone number:
2.3.4. FAX number:
2.3.5. Pager number:
2.3.6. Home telephone number (for our internal use only):
2.3.7. Secure communication channel (Yes/No):

2.4. Contact information for other site(s) involved in this incident (if available)

2.4.1. Site name:
2.4.2. Contact person name:
2.4.3. Email address:
2.4.4. Telephone number:
2.4.5. FAX number:
2.4.6. Pager number:
2.4.7. Home telephone number (for CERT/CC internal use only):
2.4.8. Secure communication channel (Yes/No):

2.5. Contact information for any other incident response team(s) (IRTs) that has/have been notified (if available)

2.5.1. IRT name:
2.5.2. Constituency domain:
2.5.3. Contact person name:
2.5.4. Email address:
2.5.5. Telephone number:
2.5.6. FAX number:
2.5.7. Pager number:
2.5.8. Home telephone number (for CERT/CC internal use only):
2.5.9. Secure communication channel (Yes/No):
2.5.10. IRT reference number:

2.6. Contact information for any law enforcement agency(ies) that has/have been notified (if available)

2.6.1. Law enforcement agency name:
2.6.2. Contact person name:
2.6.3. Email address:
2.6.4. Telephone number:
2.6.5. FAX number:
2.6.6. Pager number:

2.6.7. Home telephone number (for CERT/CC internal use only):
2.6.8. Secure communication channel (Yes/No):
2.6.9. Law enforcement agency reference number:

3.0. Contacting Sites Involved

3.1. We ask that reporting sites contact other sites involved in incident activity. Please let us know if you need assistance in obtaining contact information for the site(s) involved.

When contacting the other sites, we would very much appreciate a cc to the "cert@cert.org" alias. This helps us identify connections between incidents and understand the scope of intruder activity. We would also appreciate your including our incident number in the subject line of any correspondence relating to this incident if one has been assigned (see item 1.1.).

If you are unable to contact the involved sites, please get in touch with us to discuss how we can assist you.

3.2. Disclosure information -- may we give the following types of information to

3.2.1. the sites involved in this incident

3.2.1.1. your domain (Yes/No):
3.2.1.2. your host(s) involved (Yes/No):
3.2.1.3. your contact information (Yes/No):

3.2.2. incident response teams, for sites from their constituencies involved in this incident

3.2.2.1. your domain (Yes/No):
3.2.2.2. your host(s) involved (Yes/No):
3.2.2.3. your contact information (Yes/No):

3.2.3. law enforcement agency(ies) if there is a legal investigation

3.2.3.1. your domain (Yes/No):
3.2.3.2. your host(s) involved (Yes/No):
3.2.3.3. your contact information (Yes/No):

4.0. Host Information

4.1. Host(s) involved at your site. Please provide information on all host(s) involved in this incident at the time of the incident (one entry per host please)

4.1.1. Hostname:
4.1.2. IP address(es):
4.1.3. Vendor hardware, OS, and version:
4.1.4. Security patches applied/installed as currently recommended by the vendor and the CERT/CC (Yes/No/Unknown):
4.1.5. Function(s) of the involved host

4.1.5.1. Router (Yes/No):

4.1.5.2. Terminal server (Yes/No):
4.1.5.3. Other (e.g. mail hub, information server, DNS [external or internal], etc.):
4.1.6. Where on the network is the involved host (e.g. backbone, subnet):

4.1.7. Nature of the information at risk on the involved host (e.g., router configuration, proprietary, personnel, financial, etc.):
4.1.8. Timezone of the involved host (relative to GMT):
4.1.9. In the attack, was the host the source, the victim, or both:
4.1.10. Was this host compromised as a result of this attack (Yes/No):

4.2. Host(s) involved at other other sites (one entry per host please)

4.2.1. Hostname:
4.2.2. IP address(es):
4.2.3. Vendor hardware, OS, and version:
4.2.4. Has the site been notified (Yes/No):
4.2.5. In the attack, was the host the source, the victim, or both:
4.2.6. Was this host compromised as a result of this attack (Yes/No):

5.0. Incident Categories

5.1. Please mark as many categories as are appropriate to this incident

5.1.1. Probe(s):
5.1.2. Scan(s):
5.1.3. Prank:
5.1.4. Scam:
5.1.5. Email Spoofing:
5.1.6. Email bombardment:

5.1.6.1. was this denial-of-service attack successful (Yes/No):

5.1.7. Sendmail attack:

5.1.7.1. did this attack result in a compromise (Yes/No):

5.1.8. Break-in

5.1.8.1. Intruder gained root access (Yes/No):
5.1.8.2. Intruder installed Trojan horse program(s) (Yes/No):
5.1.8.3. Intruder installed packet sniffer (Yes/No):

5.1.8.3.1. What was the full pathname(s) of the sniffer output file(s):
5.1.8.3.2. How many sessions did the sniffer log?
(use "grep -c 'DATA' <filename>" to obtain this information):

5.1.8.4. NIS (yellow pages) attack (Yes/No):
5.1.8.5. NFS attack (Yes/No):
5.1.8.6. TFTP attack (Yes/No):
5.1.8.7. FTP attack (Yes/No):
5.1.8.8. Telnet attack (Yes/No):
5.1.8.9. Rlogin or rsh attack (Yes/No):
5.1.8.10. Cracked password (Yes/No):
5.1.8.11. Easily-guessable password (Yes/No):

5.1.9. Anonymous FTP abuse (Yes/No):
5.1.10. IP spoofing (Yes/No):
5.1.11. Product vulnerability (Yes/No):

5.1.11.1. Vulnerability exploited:

5.1.12. Configuration error (Yes/No):

5.1.12.1. Type of configuration error:

5.1.13. Misuse of host(s) resources (Yes/No):
5.1.14. Worm (Yes/No):
5.1.15. Virus (Yes/No):
5.1.16. Other (please specify):

6.0. Security Tools

6.1. At the time of the incident, were you any using the following security tools (Yes/No; How often)

Network Monitoring tools
6.1.1. Argus:
6.1.2. netlog (part of the TAMU Security Package):

Authentication/Password tools
6.1.3. Crack:
6.1.4. One-time passwords:
6.1.5. Proactive password checkers:
6.1.6. Shadow passwords: yes
6.1.7. Kerberos:

Service filtering tools
6.1.8. Host access control via modified daemons or wrappers:
6.1.9. Drawbridge (part of the TAMU Security Package):
6.1.10. Firewall (what product):
6.1.11. TCP access control using packet filtering:

Tools to scan hosts for known vulnerabilities
6.1.12. ISS:
6.1.13. SATAN:

Multi-purpose tools
6.1.14. C2 security:
6.1.15. COPS:
6.1.16. Tiger (part of the TAMU Security Package):

File Integrity Checking tools
6.1.17. MD5:
6.1.18. Tripwire:

Other tools
6.1.19. lsof:
6.1.20. cpm:
6.1.21. smrsh:
6.1.22. append-only file systems:

Additional tools (please specify):

6.2. At the time of the incident, which of the following logs were you using, if any (Yes/No)

6.2.1. syslog: yes
6.2.2. utmp: yes
6.2.3. wtmp: yes
6.2.4. TCP wrapper:
6.2.5. process accounting:

6.3. What do you believe to be the reliability and integrity of these logs (e.g., are the logs stored offline or on a different host):

7.0. Detailed description of the incident

7.1. Please complete in as much detail as possible

7.1.1. Date and duration of incident:
7.1.2. How you discovered the incident:
7.1.3. Method used to gain access to the affected host(s):
7.1.4. Details of vulnerabilities exploited that are not addressed in previous sections:
7.1.5. Other aspects of the "attack":
7.1.6. Hidden files/directories:
7.1.7. The source of the attack (if known):
7.1.8. Steps taken to address the incident (e.g., binaries reinstalled, patches applied):
7.1.9. Planned steps to address the incident (if any):
7.1.10. Do you plan to start using any of the tools listed above in question 6.0 (please list tools expected to use):
7.1.11. Other:

7.2. Please append any log information or directory listings and timezone information (relative to GMT).

7.3. Please indicate if any of the following were left on your system by the intruder (Yes/No):

7.3.1. intruder tool output (such as packet sniffer output logs):
7.3.2. tools/scripts to exploit vulnerabilities:
7.3.3. source code programs (such as Trojan horse programs, sniffer programs):
7.3.4. binary code programs (such as Trojan horse programs, sniffer programs):
7.3.5. other files:

If you answered yes to any of the last 5 questions, please call the CERT/CC hotline (+1 412 268 7090) for instructions on uploading files to us by FTP. Thanks.

7.4. What assistance would you like from the CERT/CC?

SENSITIVE SECURITY INFORMATION

FAA INFORMATION SYSTEMS SECURITY INCIDENT REPORT

Name:	**Routing Symbol:**	**Date:**
Building/Room Number:	**Date/Time Incident Discovered:**	
Type of Incident: (Virus, Personal Use, Tampering, Modifications, Theft, Other)	**City/State/Office:**	
Type of Equipment Affected:	**Sensitivity Level of Information:** (Privacy Act, Mission Critical, Nonsensitive)	

Description of Incident (User observation, events leading to discovery, organizational element affected.) (Please be specific, use reverse side if necessary)

Personnel Assigned:	**Date Assigned:**
Estimated Completion Date:	**Actual Completion Date:**
Employee Hours Used:	

Description of Action(s) Taken (Cause/Sources if Known, specific name of virus, corrective action, etc.)

FOR COMPUTER SECURITY USE ONLY

Date/Time Reported to ISSO/ISSM/ISSC	**Date/Time Reported to ACO:**
Date/Time Reported to Local Police (if necessary)	**Date/Time Reported to Other Sites:**
Personnel Action Taken: **YES/NO**	**Date Report Sent to ACS:**

SENSITIVE SECURITY INFORMATION

WARNING: THIS DOCUMENT CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER THE PROVISIONS OF 14 CFR PART 191. THE INFORMATION MAY NOT BE RELEASED IN ANY FORM WITHOUT THE EXPRESS PRIOR WRITTEN CONSENT OF THE ADMINISTRATOR OR ASSOCIATE ADMINISTRATOR FOR CIVIL AVIATION SECURITY, ACS-1. IN ACCORDANCE WITH 49 U.S.C. 40119, THIS INFORMATION IS EXEMPT BY STATUTE FROM DISCLOSURE UNDER THE FOIA. UNDER THE PROVISIONS OF 14 CFR PART 191.5(D), VIOLATORS ARE SUBJECT TO CIVIL PENALTY OR OTHER ACTION BY THE FAA.

Federal Aviation Administration

Civil Aviation Security

This document

(Document Title Here)

contains

SENSITIVE SECURITY INFORMATION (SSI).

The protective marking SENSITIVE SECURITY INFORMATION and the distribution limitation statement on this document are canceled when the attachments containing SSI are removed.

DO NOT COPY OR DISSEMINATE FURTHER.

"WARNING: THIS DOCUMENT CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER THE PROVISIONS OF 14 CFR PART 191. THE INFORMATION MAY NOT BE RELEASED IN ANY FORM WITHOUT THE EXPRESS PRIOR WRITTEN CONSENT OF THE ADMINISTRATOR OR ASSOCIATE ADMINISTRATOR OF CIVIL AVIATION SECURITY, ACS-1. IN ACCORDANCE WITH 49 USC 40119, THIS INFORMATION IS EXEMPT BY STATUTE FROM DISCLOSURE UNDER THE FOIA. UNDER THE PROVISIONS OF 14 CFR PART 191.5(D), VIOLATORS ARE SUBJECT TO CIVIL PENALTY OR OTHER ACTION BY THE FAA."

Information System Security Program
FAA Order 1600.68
Suggestion/Change Form

Dear FAA Information System User,

The information technology is ever changing. Maintaining policy and guidelines in such a dynamic environment is a challenge. The Information Systems Security Division asks your help in keeping FAA Order 1600.68 up-to-date. If you have any suggestions, comments or changes for the Information Systems Security Program, please share them with our staff. We will return a response for all submissions. Please use the Suggestion/Change Form (dated August, 1998) and send it to the address listed. The form is also available on the Civil Aviation Security web page on the FAA Intranet. The Information Systems Security Program belongs to you and your suggestions are important to us.

Thank you for your participation.

Information System Security Program
FAA Order 1600.68
Suggestion/Change Form
(August 1998)

Name:	***Region and Office Symbol:***
Address:	***Office telephone number:***
Page and Paragraph number(s):	
Narrative of suggestion(s)/change(s):	
Send Suggestion/Change Form to the Information Systems Security Division, ACO-700, through distribution or mail to: ***Office of Civil Aviation Security Operations*** ***ACO-700, Room 315*** ***800 Independence Avenue, S.W.*** ***Washington, DC 20591*** ***This form is available electronically from ACO-700 or your regional/center Security Division.***	
(ACO-700 use only) ☐ ***Adopted*** ☐ ***Not Adopted (If not adopted, explain.)***	

APPENDIX 4. SAMPLE OUTLINES AND DOCUMENTS

APPENDIX 4. SAMPLE OUTLINES AND DOCUMENTS

Evaluation Report

Each section of this sample outline of the security evaluation report is briefly described below.

1. *Introduction and Summary*. This section briefly describes the application and summarizes evaluation findings and recommendations.

2. *Background*. This section provides contextual information for the DAA. One important item is the security standards or policies that were applied. Another is a list of the general functional characteristics of the application that generically influence its certification (e.g., presence or absence of user programming). Application boundaries are defined, along with security assumptions about areas outside the boundaries.

3. *Major Finding*. The first portion of this section summarizes the controls that are in place and their general roles in protecting assets against threats and preventing exposures. This is important in maintaining perspective, and emphasizes those areas where safeguards are acceptable.

The second portion summarizes major vulnerabilities and mitigating recommendations Vulnerabilities described in the report are divided into two categories: proposed residual vulnerabilities and proposed vulnerabilities requiring correction. This format serves as both a summary of findings and a recommendation of which vulnerabilities to accept and which to correct. Authority to approve the recommendations resides with the DAA.

4. *Recommended Corrective Actions*. Corrective actions, together with anticipated costs and impacts, are recommended and prioritized. Responsibility for making the corrections might be proposed. Also, criteria must be established for evaluating the corrections. This section must be sufficiently complete to give the DAA a clear understanding of the implications of either accepting or correcting vulnerabilities.

5. *Authorization alternatives.* Other than removing an application from service or delaying its implementation, there may be intermediate authorization alternatives available. The most common is to withhold authorization pending completion of corrections. Many types of operational restrictions are also possible, such as:

a. Adding procedural security controls. Restricting use of the application to sites that have compensating controls.

b. Restricting the application to process only non-sensitive or minimally sensitive data.

c. Removing vulnerable application functions or components. (e.g., In a network environment, a weak node might be excluded from the network.)

d. Restricting users to only those with approved access to all data being processed or to those with a sufficient clearance based on an investigation. However, in an open and ever increasing global environment, this restriction may not be possible for some systems.

e. Restricting use of the application to non-critical situations where errors or failures are less severe.

f. Removing dial-up access, thus, relying more on physical security.

g. Granting conditional authorization for a limited period before full thrust is granted.

6. *Certification Process*. This section summarizes the work performed in the certification process. Its purpose is to enable the DAA to determine the confidence that can be placed in the findings. (See Chapter 2, Section 5 of this Order for further details).

7. *Attachments*. These reports describe the full set of findings, not just major ones, along with any other documents that the Certifying Authority (CA) and the DAA will need to make decisions. (See Chapter 2, Sections 4, 5, 6, and 7 of this Order for further details).

8. *Elimination of redundant reporting.* If the items discussed in paragraphs 1. through 8. of this outline already exist in other documents, such as the Information Systems Security Plan Package, attach those documents and make reference to the appropriate sections.

9. *Proposed Authorization Statement*. This is a critical part of the report. It summarizes recommended actions and is prepared for the DAA's signature. Judgments and recommendations embodied in the statement are subject to approval by the DAA. (See Chapter 2, Section 6 of this Order for further details).

This is sample outline of a system security plan. For further details, refer to the NIST document, *Guide for Developing Security Plans for Information Technology Systems.* This document is available through the Servicing Security Element (SSE) or the NIST Computer Security Resource Clearing House (Publications) on the Internet [http://csrc.nist.gov/].

Sample Security Plan Outline—Major Applications

I. SYSTEM IDENTIFICATION
- A. Responsible Organization
- B. System Name/Title
- C. System Category
- D. System Operational Status
- E. General Description/Purpose
- F. System Environment and Special Considerations
- G. System Interconnection/Information Sharing
- H. Information Contact(s)

II. SENSITIVITY OF INFORMATION HANDLED
- A. Applicable Laws or Regulations Affecting the System
- B. General Description of Sensitivity

III. SYSTEM SECURITY MEASURES
- A. Risk Assessment and Management
- B. Review of Security Controls
- C. Applicable Guidance
- D. Rules
- E. Security Control Measures
  - 1. Management Controls
    - a. Assignment of Security Responsibility
    - b. Personnel Security
  - 2. Development/Implementation Controls
    - a. Authorize Processing
    - b. Security Specifications
    - c. Design Review and Testing
  - 3. Operational Controls
    - a. Physical and Environmental Protection
    - b. Production, Input/Output Controls
    - c. Contingency Planning
    - d. Audit and Variance Detection
    - e. Application Software Maintenance Controls
    - f. Documentation
  - 4. Security Awareness and Training
    - a. Security Awareness and Training Measures
  - 5. Technical Controls
    - a. User Identification and Authentication
    - b. Authorization/Access Controls
    - c. Public Access Controls
    - d. Data Integrity/Validation Controls
    - e. Audit Trail Mechanisms
  - 6. Complimentary Controls Provided by Support System

IV. ADDITIONAL COMMENTS

Sample Security Plan Outline—General Support Systems

I. SYSTEM IDENTIFICATION
- A. Responsible Organization
- B. System Name/Title
- C. System Category
- D. System Operational Status
- E. General Description/Purpose
- F. System Environment and Special Considerations
- G. System Interconnection/Information Sharing
- H. Information Contact(s)

II. SENSITIVITY OF INFORMATION HANDLED
- A. Applicable Laws or Regulations Affecting the System
- B. General Description of Sensitivity

III. SYSTEM SECURITY MEASURES
- A. Risk Assessment and Management
- B. Review of Security Controls
- C. Applicable Guidance
- D. Rules
- E. Security Control Measures
  - 1. Management Controls
    - a. Assignment of Security Responsibility
    - b. Personnel Controls
  - 2. Acquisition/Development/Implementation Controls
    - a. Authorize Processing
    - b. Acquisition Specifications
  - 3. Operational Controls
    - a. Physical and Environmental Protection
    - b. Production, Input/Output Controls
    - c. Contingency Planning
    - d. Audit and Variance Detection
    - e. Hardware & System Software Maintenance Controls
    - f. Documentation
  - 4. Security Awareness and Training
    - a. Security Awareness and Training Measures
  - 5. Technical Controls
    - a. User Identification and Authentication
    - b. Authorization/Access Controls
    - c. Integrity Controls
    - d. Audit Trail Mechanisms
    - e. Confidentiality Controls
    - f. Incident Response Capability
  - 6. Controls Over the Security of Applications

IV. ADDITIONAL COMMENTS

Sample System Security Risk Management Plan Outline

The following outline is a sample risk management plan developed by the Volpe Center for the FAA. Although it is written for the Telecommunications Integrated Product Team (IPT), it may be used to conduct a risk assessment for any system. Further guidance on risk management may be found in Chapter 2 of this Order and the NIST Handbook, An Introduction to Computer Security, Special Publication 800-12. An electronic version of the sample risk assessment is available through the Service Security Element (SSE).

FEDERAL AVIATION ADMINISTRATION

Sample Document

SECURITY RISK MANAGEMENT PLAN
(Outline Only)

January 14, 1998

Prepared by:

U.S. Department of Transportation
Volpe National Transportation
Systems Center
Infrastructure Protection and
Operations Division, DTS-78
Cambridge, MA 02142

Prepared For:

Federal Aviation Administration
Information Systems Security
Division, ACO-700
Washington DC, 20591

TABLE OF CONTENTS

TABLES

FIGURES

APPENDICES

APPENDIX 5. MINIMUM PROTECTION REQUIREMENTS FOR EACH SECURITY LEVEL

Appendix 5
CS2 - Protection Profile Guidance for Near-Term COTS

DRAFT VERSION 0.4

by Gary Stoneburner (NIST)

Date - December 10, 1998

Revision History

Version 0.4, December 10, 1998, Protection Profile Guidance
By Gary Stoneburner (NIST)
Revision of version 0.3, adding SOF; separated threats and objectives into environment, TOE, and joint TOE/Environment; and providing information on how to use guidance in producing a "compliant" PP.

Version 0.3, July 13, 1998, Protection Profile Guidance
By Gary Stoneburner (NIST)
Revision of version 0.2, updated to CC version 2 (May 98), reflecting requirements of mutual recognition agreements (MRA), and changing from PP to PP guidance. Modifications to lists of assumptions, threats, and objectives, and to the contents of CS2-EAL are scheduled for next version.

Version 0.2, March 6, 1998, Protection Profile
By Gary Stoneburner (NIST)
Major rework of version 0.1, focusing on near-term achievability and updating to CC version 2 (Dec 98).

Version 0.1, May 23 1997, Protection Profile
By Kristina C. Rogers (Cygnacom Solutions), built to CC version 1.0. Initial version, prepared for NIST under Contract Number 50SBNB6C9287/0353-96-6308

DRAFT

TABLE OF CONTENTS

SECTION PAGE

TABLE OF TABLES
SECTION **PAGE**

1. INTRODUCTION

1.1 Identification

Title: CS2 – Guidance on PPs for Near-Term COTS

Assurance level: EAL2 – augmented (EAL-CS2)

Registration: <To be filled in upon registration>

Keywords: Protection Profile Guidance, COTS, general-purpose operating systems, applications, networked information systems, baseline protection

1.2 Overview

Purpose

The purpose of CS2 is to provide the guidance necessary to develop "compliant" protection profiles for near-term achievable, security baselines using commercial off the shelf (COTS) information technology.

CS2 accomplishes this purpose by:

- describing a largely policy-neutral, notional information system in the format of a protection profile (PP).
- specifying a subset of the common criteria to be used in developing "compliant" protection profiles
- providing the basis for refining -
  - policy neutral guidance into specific policy requirements and
  - system security threats, objectives, and requirements into a subset which is appropriate for a specific PP.

Scope

Type of system. CS2 provides the requirements necessary to specify needs for both stand-alone and distributed, multi-user information systems. This covers general-purpose operating systems, database management systems, and other applications.

Type of access. CS2 recognizes two forms of legitimate access; namely, public access and "authenticated users". With public access, the user does not have a unique identifier and is not authenticated prior to access. An example is access to information on a publicly accessible web page. Such users have legitimate access, but are differentiated from "authenticated users" who are (1) uniquely identifiable by the system, (2) have legitimate access beyond publicly available information, and (3) are authenticated prior to being granted such access.

Nature of use. CS2 "compliant" PPs are suitable for the protection of information in real-world environments, both commercial and government.

- Within government environments, CS2 "compliant" PPs are considered to be suitable for specifying the baseline protection requirements for sensitive-but-unclassified or single level classified information in an environment where all authenticated users are cleared for the level of information being processed. For classified environments, public access is not allowed into CS2 "compliant" systems. For sensitive-but unclassified environments, public access may be acceptable with additional controls, beyond Target of Evaluation (TOE) supplied mechanisms, supplied by the operational environment.

- For commercial environments, CS2 "compliant" PPs are suitable for specifying the baseline protection requirements for information in environments where all authenticated users are either (1) trusted to not maliciously attempt to circumvent nor by-pass access controls or (2) lack the motivation or capability for sophisticated penetration

attempts. Public access is allowed with environmental controls over and beyond the TOE supplied security mechanisms.

Key Assumptions. Key environmental constraints that apply for CS2 "compliant" PPs are –

- authenticated users recognize the need for a secure IT environment
- authenticated users can be reasonably trusted to correctly apply the organization's security policies in their discretionary actions
- basic physical security is provided
- competent security administration is performed
- business/mission process automation is implemented with due regard for what CS2 "compliant" PPs do not expect of their TOEs.

Summary of CS2 Requirements

Assurance. CS2 assurances have been selected to provide the level of confidence resulting from (1) existing best practices for COTS development and (2) no extensive (and hence costly) third-party evaluation. This equates, in summary, to TOE technical countermeasures that -

- are sufficient for controlling a community of benign (i.e., not intentionally malicious) authenticated users
- can provide protection against unsophisticated, technical attacks
- are not expected to protect against sophisticated, technical attacks (to include denial-of-service attacks)

Functionality. The notional CS2 system targets these user needs -

- enforcing an access control policy between active entities (subjects) and passive objects based on subject identity, allowed actions, and environmental constraints such as time-of-day and port-of-entry
- enforcing information flow control policies at the macro (e.g., domain to domain) level
- resistance to resource depletion by providing resource allocation features
- providing mechanisms to detect some insecurities
- providing mechanisms for trusted recovery in the event of some system failures or detected insecurities
- supporting these capabilities in a distributed system connected via an untrusted network

CS2 "compliant" PPs are not expected to require that the TOE –

- provide the label-based controls appropriate for protecting controlled information (such as government classified, company proprietary, or export restricted data) in environments containing authenticated users who are not allowed access to such information
- protect against malicious abuse of authorized privileges
- provide sufficient protection against installation, operation, or administration errors

2. TOE DESCRIPTION

This section describes the CS2 class of protection profiles (PPs) in terms of the TOEs covered. These TOEs are identified by class of products, the operational environment, and the required security functionality.

2.1 Product Class

CS2 provides PP guidance for PPs which include general-purpose operating systems and applications in both stand-alone and networked environments. The TOEs covered by such PPs permit one or more processors and attached peripheral and storage devices to be used by multiple users to perform a variety of functions requiring controlled, shared access to processing capability and information.

The TOE may be (1) a stand-alone system, (2) a distributed system, or (3) confined to a single host but intended to interface with a networked environment. The TOE will provide user services directly or serve as a platform for compliant applications. Unless explicitly stand-alone, the TOE will support protected communications across an untrusted network; unless of course, the network is a part of the TOE.

2.2 Operational Environment

The TOE supports the active entities of human users and software processes. Human users, in conjunction with system processes, are accountable for all system activities. The TOE generates processes that act on behalf of either a specific human user or a uniquely identifiable system process. A process requests and consumes resources on behalf of its unique, associated user or system process. In a networked environment, a process may invoke another process on a different system.

A distributed TOE, or a TOE intended for use in a networked environment, will support one or more types of communication and protocols, such as:

- Synchronous process communication; e.g., remote procedure calls (RPC)
- Asynchronous process communication; e.g., message passing using user datagram protocol (UDP)
- Electronic mail; e.g., simple mail transfer protocol (SMTP)
- Dedicated network services; e.g., hypertext transfer protocol (HTTP)
- Network management protocols; e.g., simple network management protocol (SNMP)

A compliant TOE will generally support –

- Users with networked access to the TOE across an untrusted network (that is, mechanisms operating within the TOE cooperate with mechanisms in other components to securely exchange information across an untrusted network)
- Several users executing tasks on the same system concurrently
- Sharing resources, such as printer and mass storage, across a network

2.3 Required Security Functionality

CS2 specifies the requirements for a system with the security functionality listed below. A specific CS2 "compliant" PP will call out that subset of this functionality which is appropriate for the specific environment and type of TOE it covers.

- Executing the access control policy of the imposed IT security policy
- Assigning a unique identifier to each authenticated user
- Assigning a unique identifier to each system process, including those not running on behalf of a human user (e.g., processes started at system bootup like the Unix "inetd")

- Authenticating the claimed user identity before allowing any user to perform any actions other than a well-defined set of operations (e.g., reading from a public web site)
- Auditing in support of individual accountability and detection of and response to insecurity
- Enabling access authorization management; i.e., the initialization, assignment, and modification of access rights (e.g. read, write, execute) to data objects with respect to (1) active entity name or group membership and (2) environmental constraints such as time-of-day and port-of-entry.
- Resource allocation features providing a measure of resistance to resource depletion
- Mechanisms for detecting some insecurities
- System recovery features providing a measure of survivability in the face of system failures and insecurities
- Automated support to help in the verification of secure delivery, installation, operation, and administration

3. SECURITY ENVIRONMENT

{Editorial note: Work is still required to produce assumptions and threats with broad consensus.}

3.1 Introduction

This section identifies the following:

- significant assumptions about the operational environment for CS2 "compliant" PPs
- organizational security policies for which CS2 compliant PPs are appropriate
- IT-related threats to the organization countered by the information technology in the notional CS2 information system
- threats requiring reliance on environmental controls to provide sufficient protection
- general description of the assurance required for CS2

By providing the information describe above, this section gives the basis for the security objectives described in section 4 and hence the specific security requirements listed in sections 5 and 6.

3.2 Secure Usage Assumptions

The specific conditions listed below are assumed to exist in a CS2 environment. These assumptions include both practical realities to be considered in the development of security requirements in CS2 "compliant" PPs and essential environmental constraints on the use of TOEs compliant with such a PP.

Table 3.2-1 – Security assumptions

Type	Name	Assumption	Discussion
Physical	A.PHYSICAL	The processing resources of the TOE that depend on hardware security features will be located within controlled access facilities that mitigate unauthorized, physical access.	A TOE will not be able to meet its security requirements unless at least a minimum degree of physical security is provided.
Personnel	A.USER-NEED	Authenticated users recognize the need for a secure IT environment.	It is essential that the authenticated users appreciate the need for security. Otherwise they are likely to try and circumvent it.
	A.USER-TRUST	Authenticated users are generally trusted to perform discretionary actions in accordance with security policies.	Authenticated users will have a fair amount of discretion with CS2 systems. It is important that they be adequately trained and motivated to make wise choices in these actions. This "trust" is not absolute, but must be a reasonable expectation. Hence the phrase "generally trusted"
	A. ADMIN	The security features of the TOE are competently administered on an on-going basis.	It is essential that security administration be both competent and on-going.

3.3 ORGANIZATIONAL SECURITY POLICIES

The organizational security policies discussed below are addressed by the notional CS2 information system.

Table 3.3-1 – Security policies

Name	Policy	Discussion
P.ACCESS	Access rights to specific data objects are determined by object attributes assigned to that object, user identity, user attributes, and environmental conditions as defined by the security policy.	CS2 supports organizational policies which grant or deny access to objects using rules driven by attributes of the user (such as user identity, group, etc.), attributes of the object (such as permission bits), type of access (such as read or write), and environmental conditions (such as time-of-day).
P.INFO-FLOW	Information flow between IT components must be in accordance with established information flow policies.	CS2 includes information flow control as this is needed in many environments. Whether this is a part of a specific PP depends upon the policy that PP is intending to cover.
P.ACCOUNT	Users must be held accountable for security-relevant actions.	CS2 supports organizational policies requiring that users are held accountable for their actions, facilitating after-the-fact investigations and providing some deterrence to improper actions.
P.KNOWN	Except for a well-defined set of allowed operations, users of the TOE must be identified and authenticated before TOE access can be granted.	Beyond a well-defined set of actions such as read access to a public web-server, there is a finite community of known, authenticated users who are authenticated before being allowed access.
P.TRAINING	Authenticated users of the system must be adequately trained, enabling them to (1) effectively implement organizational security policies with respect to their discretionary actions and (2) support the need for non-discretionary controls implemented to enforce these policies.	Once granted legitimate access, authenticated users are expected to use IT resources and information only in accordance with the organizational security policy. In order for this to be possible, these users must be adequately trained both to understand the purpose and need for security controls and to be able to make secure decisions with respect to their discretionary actions.
P.SURVIVE	The IT system, in conjunction with its environment, must be resilient to insecurity, resisting the insecurity and/or providing the means to detect an insecurity and recover from it.	CS2 systems will provide a measure of this resilience through functionality and assurances that resist, detect, and recover from insecurities. For sophisticated attacks, a large portion of this resilience is provided by the TOE environment.
P.USAGE	The organization's IT resources must be used for only for authorized purposes.	CS2 systems must, in conjunction with its environment, ensure that the organization's information technology is not used for unauthorized purposes.
P.DUE-CARE	The organization's IT systems must be implemented and operated in a manner that represents due care and diligence with respect to risks to the organization.	It is important that the level of security afforded the IT system be in accordance with what is generally considered adequate within the business or government sector in which the organization is placed.

Name	Policy	Discussion
P.COMPLY	The implementation and use of the organization's IT systems must comply with all applicable laws, regulations, and contractual agreements imposed on the organization.	The organization will meet all requirements imposed upon it from the outside; for example: government regulations, national and local laws, and contractual agreements.
P.NETWORK	The organization's IT security policy must be maintained in the environment of distributed systems interconnected via insecure networking.	Since CS2 systems will likely be interconnected across untrusted networking, this policy statement will have a significant impact on CS2 requirement definition.

3.4 Threats to Security

The technical countermeasures of the notional CS2 system are required to counter threats which may be broadly categorized as -

- the threat of unsophisticated, malicious attacks from individuals other than authenticated users
- the threat of authenticated users attempting, non-maliciously to gain unauthorized access or to perform an unauthorized operation. Such attempts may be performed to "get the job done", out of curiosity, as a challenge, or as a result of an error.

Other threats that can affect system security must be dealt with in conjunction with controls provided by the operating environment.

The threats facing CS2 systems are listed in Tables 3.4-1 through 3.4-3 and discussed further in sections 3.4.1 through 3.4.3 as follows:

3.4-1 and 3.4.1: Threats addressed by the environment

3.4-2 and 3.4.2: Threats addressed by the TOE

3.4-3 and 3.4.3: Threats addressed jointly by the TOE and its environment

Threats addressed by the TOE's environment

It is expected that all CS2 "compliant" PPs will include the threats listed in Table 3.4-1. In addition, since a specific PP narrows the scope to a specific IT product within the system, that PP will likely add to this list threats from Tables 3.4-2 and 3.4-3. These added threats represent what will be satisfied by the IT, other than the TOE, in the notional CS2 system. (In the CS2 "compliant" PP, sections 3.4.1 through 3.4.3 will be adjusted to correspond to these changes in Tables 3.4-1 through 3.4-3. Additionally, these changes must be reflected in Section 4 "Security Objectives" of the "compliant" PP.)

Table 3.4-1 – Security threats addressed by TOE's Environment

T.PHYSICAL	Security-critical parts of the TOE may be subjected to a physical attack that may compromise security.
T.ENTRY-SOPHISTICATED	An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.
T.ENTRY-NON-TECHNICAL	An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.
T.ACCESS-NON-TECHNICAL	An authenticated user may gain non-malicious, unauthorized access using non-technical means.
T.DENIAL-SOPHISTICATED	The system may be subjected to a sophisticated, denial-of-service attack.

Threats addressed by the TOE

While all of the threats listed in Table 3.4-2 will appear in a CS2 "compliant" PP, that PP will tailor these threats to the specifics of the operational environment being addressed and the nature of the TOE within that environment. This is done by moving threats that are not addressed by that TOE into Table 3.4-1 (threats addressed by the environment) and moving threats addressed jointly by that TOE and the remaining IT in the notional CS2 system into Table 3.4-3 (jointly addressed threats). (In the CS2 "compliant" PP, sections 3.4.1 through 3.4.3 will be adjusted to correspond to these

changes to Tables 3.4-1 through 3.4-3. Additionally, these changes must be reflected in Section 4 “Security Objectives” of the “compliant” PP.)

Table 3.4-2 – Security threats addressed by TOE

Name	Threat
T.ACCESS	An authenticated user may gain unauthorized, non-malicious access to a resource or to information via user error, system error, or an unsophisticated, technical attack.
T.CRASH	The secure state of the TOE could be compromised in the event of a system crash.
T.ENTRY	An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information via an unsophisticated, technical attack.
T.OBSERVE	Events occur in TOE operation that compromise IT security but the TOE , due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.
T.RECORD-EVENT	Security relevant events may not be recorded.
T.TRACEABLE	Security relevant events may not be traceable to the user or system process associated with the event.
T.AUDIT-CORRUPTED	Records of security events may be subjected to unauthorized modification or destruction.
T.AUDIT-CONFIDENTIALITY	Records of security events may be disclosed to unauthorized individuals or processes.
T.RESOURCES	The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.
T.DENIAL	The TOE may be subjected to an unsophisticated, denial-of-service attack.

Threats addressed jointly by the TOE and its environment

In a specific CS2 "compliant" PP, the TOE (as a subset of the overall, notional CS2 system) may not be able to help address some of the threats listed in Table 3.4-3. In that case such threats would be moved into Table 3.4-1 (threats addressed by the environment) for that PP. It is also possible that PP author may decide to specify the nature of compliant solutions more stringently than this CS2 PP guidance has done. It that case some of the jointly addressed threats may become either a TOE addressed threat and be moved into Table 3.4-2 or an environmental addressed threat and be moved into Table 3.4-1. (In the CS2 "compliant" PP, sections 3.4.1 through 3.4.3 will be adjusted to correspond to these changes to Tables 3.4-1 through 3.4-3. Additionally, these changes must be reflected in Section 4 "Security Objectives" of the "compliant" PP.)

Table 3.4-3 – Security threats addressed Jointly by TOE and Environment

T.INSTALL	The TOE may be delivered or installed in a manner that undermines security.
T.OPERATE	Security failures may occur because of improper operation of the TOE; e.g., the abuse of authorized privileges.
T.ACCESS-MALICIOUS	An authenticated user may obtain unauthorized access for malicious purposes.
T.ADMIN-ERROR	The security of the TOE may be reduced or defeated due to errors or omissions in the administration of the security features of the TOE.
T.SYSTEM-CORRUPTED	The security state of the TOE, as a result of another threat, may be intentionally corrupted to enable future insecurities.

3.4.1 Threats environment addresses

The threats discussed below must be countered but are not addressed by the technical countermeasures within the notional CS2 system. Such threats must therefore, be addressed in conjunction with the operating environment.

T.PHYSICAL: Security-critical parts of the TOE may be subjected to a physical attack that may compromise security.

The security offered by CS2 can be assured only to the extent that the hardware and software relied upon to enforce the security policy is physically protected from unauthorized physical modification and from technical attacks at the hardware level. Examples of such attacks are using electromagnetic pulse weapons, intercepting radiated electronic emissions, and passive monitoring or active attacking of physical transmission medium (e.g., coax, twisted-pair, or fiber optic cable).

T.ENTRY-SOPHISTICATED: An individual, other than an authenticated user, may gain access to processing resources or information using a sophisticated, technical attack.

The TOE is not required to protect against sophisticated, technical attacks. There is no reasonable expectation that a TOE compliant with a CS2 PP will significantly increase, over that associated with a non-compliant TOE, the work-factor required to accomplish a successful, high-grade attack. Therefore, this threat is largely addressed by the TOE environment.

T.ENTRY-NON-TECHNICAL: An individual, other than an authenticated user, may gain access to processing resources or information using non-technical means.

T.ACCESS-NON-TECHNICAL: An authenticated user may gain non-malicious, unauthorized access using non-technical means.

The use of non-technical attack means; for example, social engineering or dumpster diving; is beyond the scope of TOE protections and must be addressed by the environment.

T.DENIAL-SOPHISTICATED: The system may be subjected to a sophisticated, denial-of-service attack.

The TOE is not capable of resisting sophisticated attacks and must therefore, rely on protections provided by its environment to maintain availability in the face of such threats.

3.4.2 Threats TOE addresses

Technical countermeasures within the notional CS2 system address the threats discussed below.

T.ACCESS: An authenticated user may gain unauthorized, non-malicious access to a resource or to information via user error, system error, or an unsophisticated, technical attack.

An authenticated user is someone who is (1) uniquely identifiable by the system, (2) has legitimate access beyond publicly available information, and (3) is authenticated prior to being granted such access.

By virtue of having access, the threat posed from authenticated users is inherently greater than that posed from unauthorized individuals. CS2 systems are required to have only the assurances necessary to cover the threat of non-malicious actions by authenticated users; i.e., sufficient confidence in light of the fact that only non-malicious actions are covered.

There are two broad categories of users with respect to this threat:

- The first category are persons who possess little technical skills, do not have access to sophisticated attack tools, and, because they have some rights of access, are mostly trusted not to attempt to maliciously subvert the system nor maliciously exploit the information stored thereon. Users in this category may be motivated by curiosity to gain access to information for which they have no authorization.

- The second category of users is technically skilled or has access to sophisticated attack tools and some may attempt to bypass system controls as a technical challenge or as a result of curiosity. CS2 compliant components and systems would generally be used in environments where these users are highly trusted not to attempt to maliciously subvert the system nor to maliciously exploit the information stored thereon.

T.CRASH: The secure state of the TOE could be compromised in the event of a system crash.

For the TOE to protect the information it controls, it must remain in a secure state, including after recovery from a system failure or discontinuity of service.

System crash can occur with inadequate mechanisms for secure recovery. User data objects and audit information may be modified or lost and system or application software may corrupted.

T.ENTRY: An individual other than an authenticated user may gain unauthorized, malicious access to processing resources or information via an unsophisticated, technical attack.

The mechanisms and assurances of a TOE compliant with a CS2 PP will resist low-grade technical attacks. (Resistance to higher-grade attacks, when such resistance is required, must be provide by the TOE operational environment.)

T.OBSERVE: Events occur in TOE operation that compromise IT security but the TOE , due to flaws in its specification, design, or implementation, may lead a competent user or security administrator to believe that the system is still secure.

This is the threat of an administrator or user not detecting a security problem because of errors or omissions in the TOE's human interface. The TOE is then used in a manner which is insecure but which the administrator or user reasonably, but incorrectly, believes to be secure.

T.RECORD-EVENT: Security relevant events may not be recorded.

T.TRACEABLE: Security relevant events may not be traceable to the user or system process associated with the event.

T.AUDIT-CORRUPTED: Records of security events may be subjected to unauthorized modification or destruction.

T.AUDIT-CONFIDENTIALITY: Records of security events may be disclosed to unauthorized individuals or processes.

TOE security depends in part on the ability of the TOE to detect and report the occurrence of security relevant events, to determine the identity of those responsible for such events, and to protect the event records from unauthorized access, modification, or destruction.

T.RESOURCES: The shared, internal TOE resources may become exhausted due to system error or non-malicious user actions.

System availability depends partly on the availability of shared resources.

T.DENIAL: The TOE may be subjected to an unsophisticated, denial-of-service attack.

The system must be able to withstand unsophisticated denial-of-service attacks.

3.4.3 Threats TOE and Environment jointly address

T.INSTALL: The TOE may be delivered or installed in a manner that undermines security.

The security offered by CS2 is predicated upon the TOE being initially established in a secure state. That includes assurance that the TOE delivered is that which was evaluated and that the TOE is subsequently installed properly. While the TOE is expected to provide mechanisms to support mitigating against this threat, the support of the environment is critical.

T.OPERATE: Security failures may occur because of improper operation of the TOE; e.g., the abuse of authorized privileges.

The security offered by CS2 can be assured only to the extent that the TOE is operated correctly by system administrators and authenticated users in accordance with security policy. The TOE will provide mechanisms that help mitigate this threat. Yet specific environmental controls are also required.

T.ACCESS-MALICIOUS: An authenticated user may obtain unauthorized access for malicious purposes.

CS2 functionality and assurances are sufficient mitigation for non-malicious actions by authenticated users. The greater risk from malicious actions by authenticated users must be addressed in conjunction with the environment.

T.ADMIN-ERROR: The security of the TOE may be reduced or defeated due to errors or omissions in the administration of the security features of the TOE.

Authenticated users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE which permit them to gain unauthorized access.

This threat is only partly covered by the TOE and therefore must also be addressed by the TOE environment.

T.SYSTEM-CORRUPTED: The security state of the TOE, as a result of another threat, may be intentionally corrupted to enable future insecurities.

The TOE security depends to a large degree on the integrity of the hardware and software implementing the security functionality. If this is intentionally corrupted, the TOE will be unable to maintain a secure state. The TOE can only partially protect against this threat.

3.5 General Assurance Need

CS2 “compliant” PPs are targeted for near-term achievable, cost-effective, COTS security. In keeping with this target, the general level of assurance for CS2 must:

- be consistent with current best commercial practice for IT development and
- enable evaluated products that are competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.

CS2 assurance must also, to enhance wide-spread acceptance, be consistent with current and near-term mutual recognition arrangement. This requires that the CS2 assurances:

- be expressed as an existing evaluation assurance level (EAL) from part 3 of the Common Criteria; augmented by CC assurance components as required
- contain no assurance components first appearing in EAL5 or above

In keeping with these requirements, the general level of assurance needed for CS2 is EAL2 augmented to include other vendor actions within the scope of current best commercial practice.

4. SECURITY OBJECTIVES

{Editorial note: Work is still required to produce objectives with broad consensus.}

4.1 Environmental Security Objectives

Addressing some policies and threats is beyond the capabilities of the notional CS2 system. These result in the objectives listed in Table 4-1. The CS2 system does not contribute significantly to meeting these objectives.

It is expected that all CS2 "compliant" PPs will list these environmental objectives. In addition, since a specific PP narrows the scope to a specific IT product within the system, that PP will likely add to this list objectives from Tables 4.2 and 4.3. These added objectives represent what will be satisfied by the IT, other than the TOE, in the notional CS2 system. (These changes must be consistent with the threat categorizations in section 3.4 "Threats to Security" of the "compliant" PP.)

Table 4-1 – Environmental Security Objectives

Environmental Security Objective	Corresponding Threat or Policy
O.PHYSICAL: Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from physical attack that might compromise IT security.	T.PHYSICAL
O.ACCESS-MALICIOUS: The TOE environment must sufficiently mitigate the threat of malicious actions by authenticated users.	T.ACCESS-MALICIOUS
O.ENTRY-SOPHISTICATED: The TOE environment must sufficiently mitigate the threat of an individual (other than an authenticated user) gaining unauthorized access via sophisticated, technical attack.	T.ENTRY-SOPHISTICATED
O.ACCESS-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by authenticated users for non-malicious purposes.	T.ACCESS-NON-TECHNICAL
O.ENTRY-NON-TECHNICAL: The TOE environment must provide sufficient protection against non-technical attacks by other than authenticated users.	T.ENTRY-NON-TECHNICAL
O.DETECT-SOPHISTICATED: The TOE environment must provide the ability to detect sophisticated attacks and the results of such attacks (e.g., corrupted system state).	P.SURVIVE T.SYSTEM-CORRUPTED
O.DENIAL-SOPHISTICATED: The TOE environment must maintain system availability in the face of sophisticated denial-of-service attacks.	P.SURVIVE T.DENIAL-SOPHISTICATED

4.2 TOE Security Objectives

While the environment contributes to the satisfaction of nearly all objectives, those listed here are satisfied by the TOE with only generic environmental support such as user training.

Table 4-1 gives the security objectives to be met by the notional CS2 information system.

While all of the TOE objectives will appear in a CS2 "compliant" PP, that PP will tailor these objectives to the specifics of the operational environment being addressed and the nature of the TOE within that environment. This is done by

moving objectives that are not addressed by that TOE into Table 4-1 (environmental objectives) and moving objectives addressed jointly by that TOE and the remaining IT in the notional CS2 system into Table 4-3 (joint objectives). (These changes must be consistent with the threat categorizations in section 3.4 "Threats to Security" of the "compliant" PP.)

Table 4-2 – TOE Security Objectives

IT Security Objective	Corresponding Threat or Policy
O.ACCESS: The TOE must provide public access and access by authenticated users to those TOE resources and actions for which they have been authorized.	P.ACCESS
O.INFO-FLOW: The TOE must ensure that any information flow control policies are enforced - (1) between TOE components and (2) at the TOE external interfaces.	P.INFO-FLOW
O.KNOWN: The TOE must ensure that, except for a well-defined set of allowed actions, all users are identified and authenticated before being granted access.	P.KNOWN
O.AUTHORIZE: The TOE must provide the ability to specify and manage user and system process access rights to individual processing resources and data elements, supporting the organization's security policy for access control. NOTE: This includes initializing, specifying and managing (1) object security attributes, (2) active entity identity and security attributes, and (3) security relevant environmental conditions.	P.ACCESS
O.ACCOUNT: The TOE must ensure that all TOE users can subsequently be held accountable for their security relevant actions.	P.ACCOUNT T.TRACEABLE T.RECORD-EVENT T.AUDIT-CORRUPTED T.AUDIT-CONFIDENTIALITY
O.BYPASS: The TOE must prevent errant or non-malicious, authorized software or users from bypassing or circumventing TOE security policy enforcement. NOTE: This objective is limited to 'non-malicious' because CS2 controls are not expected to be sufficient mitigation for the greater negative impact that 'malicious' implies.	T.ACCESS
O.ENTRY: The TOE must prevent logical entry to the TOE using unsophisticated, technical methods, by persons without authority for such access.	P.USAGE T.ENTRY
O.OBSERVE: The TOE must ensure that its security status is not misrepresented to the administrator or user.	T.OBSERVE
O.RECOVER: The TOE must provide for recovery to a secure state following a system failure, discontinuity of service, or detection of an insecurity.	P.SURVIVE T.CRASH

IT Security Objective	Corresponding Threat or Policy
O.DETECT: The TOE must enable the detection of insecurities. Note: The level of detection provided by the TOE is only that corresponding to the level of attack sophistication being protected against by the other IT-objectives.	P.SURVIVE T.SYSTEM-CORRUPTED
O.AVAILABLE: The TOE must protect itself from unsophisticated, denial-of-service attacks.	P.SURVIVE T.DENIAL
O.RESOURCES: The TOE must protect itself from user or system errors that result in shared resource exhaustion.	P.SURVIVE T.RESOURCES
O.NETWORK: Unless explicitly stand-alone, the TOE must be able to meet its security objectives in a distributed environment. This may be either as a distributed TOE and as a TOE networked with other IT resources.	P.NETWORK

4.3 Joint TOE/Environment Security Objectives

The objectives listed here fall into one or more of the following categories:

a. The TOE and its environment together satisfy the objective as follows:

(1) TOE - contributes in a significant manner and

(2) Environment - contribution is specific to this objective; i.e, not the result of a general contribution such as user training.

b. At the level of abstraction of the PP either:

(1) It is not possible to accurately determine the split between TOE and environmental contribution, or

(2) Multiple, compliant solutions are feasible resulting in different mixes of TOE and environmental contributions

In a specific CS2 "compliant" PP, the TOE (as a subset of the overall, notional CS2 system) may not provide support for some of these objectives. In that case such objectives would be moved into Table 4-1 (environmental objectives) for that PP. It is also possible that PP author may decide to specify the nature of compliant solutions more stringently than this CS2 PP guidance has done. It that case some of the joint objectives may become either a TOE objective and be moved into Table 4-2 (TOE objectives) or an environmental objective and be moved into Table 4-1 (environmental objectives). (These changes must be consistent with the threat categorizations in section 3.4 "Threats to Security" of the "compliant" PP.)

Table 4-3 – Joint TOE/Environment Security Objectives

Joint Security Objective	Corresponding Threat or Policy
O.OPERATE: Those responsible for the TOE (in conjunction with mechanisms provided by the TOE) must ensure that the TOE is delivered, installed, and operated in a manner which maintains IT security.	T.INSTALL T.OPERATE P.TRAINING
O.MANAGE: Those responsible for the TOE (in conjunction with mechanisms provided by the TOE) must ensure that it is managed and administered in a manner that maintains IT security.	T.ADMIN-ERROR
O.COMPLY: The TOE environment, in conjunction with controls implemented by the TOE, must support full compliance with applicable laws, regulations, and contractual agreements.	P.COMPLY
O.DUE-CARE: The TOE environment, in conjunction with the TOE itself, must be implemented and operated in a manner that clearly demonstrates due-care and diligence with respect to IT-related risks to the organization.	P.DUE-CARE

5. Functional Security REQUIREMENTS

This section contains the functional requirements that must be satisfied by the notional CS2 system. A specific CS2 compliant PP will tailor these requirements to the specifics of the operational environment being addressed and the nature of the TOE within that environment. These requirements consist of functional components from Part 2 of the CC, in some cases with modifications.

This protection profile (PP) guidance is designed to be largely policy-neutral. Therefore, most policy-related assignments and selections are deferred to the PP for explicit specification. Where the policy is sufficiently generic, it is specified in this PP guidance and not deferred.

5.1 Functional Requirements - TOE

Table 5-1 lists the functional requirements for the notional CS2 information system and the security objectives each requirement helps to address. All functional and assurance dependencies associated with the components in Table 5-1 have been satisfied.

Appendix B contains the explicit functional requirements that are summarized here.

As described in sections 3.4 “Threats to Security” and 4. “Security Objectives”, for a specific, CS2 “compliant” PP, some of the system security needs will not be met by the TOE of that PP. As indicated in section 5.3, these unmet IT requirements become requirements on the IT environment surrounding the TOE and are moved from Table 5-1 into Table 5-2. (The requirements moved from Table 5-1 into Table 5-2 must correspond with the changes made to the CS2 guidance categorization of threats and objectives in sections 3.4 and 4 of the “compliant” PP.)

Table 5-1 – Functional Components - TOE

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
1	FAU_GEN.1	Audit data Generation	x		x	O.ACCOUNT O.RECOVER O.DETECT O.OPERATE O.MANAGE O.DUE-CARE
2	FAU_GEN.2	User Identity Generation		x		O.ACCOUNT
3	FAU_SAR.1	Audit Review			x	Required dependency for: FAU_SAR.2 FAU_SAR.3
4	FAU_SAR.2	Restricted Audit Review				O.BYPASS

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
5	FAU_SAR.3	Selectable Audit Review			x	O.ACCOUNT O.RECOVER O.DETECT O.DUE-CARE O.OPERATE O.MANAGE O.COMPLY
6	FAU_SEL.1	Selective Audit	x		x	O.DUE-CARE O.DETECT O.MANAGE O.OPERATE O.COMPLY
7	FAU_STG.1	Protected audit trail storage				O.DETECT O.DUE-CARE O.COMPLY O.ACCOUNT O.BYPASS
8	FAU_STG.3	Action in case of Possible Audit Data Loss			x	O.ACCOUNT O.DUE-CARE O.MANAGE
9	FDP_ACC.1	Subset Access Control			x	O.ACCESS O.ENTRY O.DUE-CARE O.COMPLY O.AVAILABLE O.RESOURCES
10	FDP_ACF.1	Security Attribute Based Access Control	x		x	O.ACCESS O.ENTRY O.DUE-CARE O.COMPLY O.AVAILABLE O.RESOURCES

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
11	FDP_DAU.1	Basic data authentication			x	O.BYPASS O.DUE-CARE O.ENTRY O.AVAILABLE
12	FDP_ETC.1	Export of user data without security attributes			x	O.BYPASS O.DUE-CARE O.ENTRY O.AVAILABLE
13	FDP_IFC.1	Subset information flow control			x	Required dependency for: FDP_IFF.1 FDP_IFF.8
14	FDP_IFF.1	Simple security attributes			x	O.INFO-FLOW O.COMPLY O.DUE-CARE
15	FDP_ITC.1	Import of user data without security attributes			x	O.NETWORK
16	FDP_ITT.1	Basic internal transfer protection			x	O.NETWORK
17	FDP_RIP.1	Subset Residual Information protection			x	O.BYPASS O.DUE-CARE
18	FDP_SDI.1	Stored data integrity monitoring			x	O.DETECT O.RECOVER
19	FDP_UCT.1	Basic data exchange confidentiality			x	O.NETWORK
20	FDP_UIT.1	Data exchange integrity			x	O.NETWORK
21	FIA_AFL.1	Authentication Failure Handling		x	x	O.DETECT O.ENTRY O.BYPASS O.DUE-CARE O.COMPLY
22	FIA_ATD.1	User Attribute Definition			x	O.AUTHORIZE
23	FIA_SOS.1	Verification of Secrets			x	O.BYPASS O.DUE-CARE O.COMPLY

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
24	FIA_SOS.2	TSF Generation of Secrets			x	O.BYPASS O.DUE-CARE O.COMPLY
25	FIA_UAU.1	Timing of authentication			x	O.KNOWN
26	FIA_UAU.5	Multiple authentication mechanisms			x	O.NETWORK
27	FIA_UAU.6	Re-authenticating			x	O.BYPASS
28	FIA_UAU.7	Protected authentication feedback				O.BYPASS
29	FIA_UID.1	Timing of identification			x	O.KNOWN
30	FIA_USB.1	User-Subject Binding				O.ACCESS O.DUE-CARE O.BYPASS
31	FMT_MOF.1	Management of security functions behavior			x	O.MANAGE O.DUE-CARE
32	FMT_MSA.1	Management of security attributes			x	O.MANAGE O.DUE-CARE O.AUTHORIZE
33	FMT_MSA.3	Static attribute initialization			x	O.MANAGE O.DUE-CARE O.AUTHORIZE
34	FMT_MTD.1	Management of TSF data			x	O.MANAGE O.DUE-CARE
35	FMT_SAE.1	Time-Limited Authorization			x	O.ACCESS O.ENTRY O.AUTHORIZE O.MANAGE O.DUE-CARE
36	FMT_SMR.1	Security roles			x	O.MANAGE O.DUE-CARE
37	FPT_AMT.1	Abstract Machine Testing			x	Required dependency for: FPT_TST.1
38	FPT_FLS.1	Failure with preservation of secure state			x	O.RECOVER

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
39	FPT_ITC.1	Inter-TSF Confidentiality During Transmission		x	x	O.NETWORK
40	FPT_ITI.1	Inter-TSF detection of modification		x	x	O.NETWORK
41	FPT_ITT.1	Basic internal TSF data transfer protection		x	x	O.NETWORK
42	FPT_RCV.1	Manual Recovery				O.RECOVER
43	FPT_RPL.1	Replay detection			x	O.NETWORK
44	FPT_RVM.1	Non-Bypassability of the TSP				O.BYPASS
45	FPT_SEP.1	TSF Domain Separation				O.BYPASS O.DUE-CARE
46	FPT_TDC.1	Inter-TSF basic TSF data consistency		x	x	O.NETWORK
47	FPT_TRC.1	Internal TSF consistency			x	O.NETWORK
48	FPT_TST.1	TSF Testing			x	O.DETECT O.DUE-CARE
49	FRU_RSA.1	Maximum quotas			x	O.RESOURCES
50	FTA_LSA.1	Limitation on scope of selectable attributes			x	O.ACCESS O.ENTRY O.DUE-CARE
51	FTA_MCS.1	Basic limitation on multiple concurrent session		x	x	O.ACCESS O.ENTRY O.DUE-CARE
52	FTA_SSL.1	TSF-initiated session locking		x		O.BYPASS O.DUE-CARE
53	FTA_SSL.2	User-initiated locking				O.OPERATE O.BYPASS O.DUE-CARE
54	FTA_SSL.3	TSF-initiated termination		x		O.BYPASS O.DUE-CARE
55	FTA_TAB.1	Default TOE access banners		x		O.ENTRY O.ACCOUNT O.DUE-CARE O.COMPLY

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address
56	FTA_TAH.1	TOE access history				O.OBSERVE O.ENTRY O.BYPASS O.DUE-CARE O.COMPLY
57	FTA_TSE.1	TOE session establishment		x	x	O.ACCESS O.ENTRY
58	FTP_ITC.1	Inter-TSF trusted channel		x	x	O.NETWORK
59	FTP_TRP.1	Trusted path		x	x	O.NETWORK
60	Non-CC FPT_CS2.1	TSF synchronization FPT_STM.1 changed to be synchronization requirements (instead of just requiring a mechanism that supports it)	x			O.NETWORK

5.2 Functional Requirements - IT Environment

This section describes what is known about the functional requirements that the IT in the environment surrounding the TOE must provide in order for the environmental and joint security objectives to be met.

Since the TOE for this CS2 PP guidance document is the entire, notional CS2 system - Table 5-2 is currently empty. However, in a specific, CS2 "compliant" PP this section will provide the requirements which must be met by the IT surrounding the TOE. This is be accomplished by moving the requirements from Table 5-1 which are not met by the TOE of that PP into Table 5-2 below. (The requirements moved from Table 5-1 into Table 5-2 must correspond with the changes made to the CS2 guidance categorization of threats and objectives in sections 3.4 and 4 of the "compliant" PP.)

Table 5-2 – Functional Components - IT Environment

Req Number	CC Component	Name	Extended	Refined	ST adds detail	Objectives function helps address

5.3 Non-IT Environmental Functional Requirements

The environment is required to satisfy the secure usage assumptions in Section 3.1 and to meet all of the environmental security objectives outlined in section 4.1 and support the objectives in section 4.3. The specific, non-IT functional requirements are not identified in this PP. The higher-level objective statements are considered sufficient for determining the adequacy of non-IT environmental support.

To the extent that the non-IT environment surrounding the notional CS2 system is the same as that surrounding the TOE in a specific, CS2 "compliant" PP, the expectations toward the non-IT environment will not change from PP to PP.

5.4 Strength of Function (SOF)

This section is required by the Common Criteria and specifies the strength of function necessary to accomplish the intent of this PP. Both a minimum level for the PP as a whole and specific metrics for individual functions are provided.

5.4.1 Minimum SOF Requirement

As the goal for CS2 is near-term achievable COTS, the appropriate minimum SOF level is **BASIC**.

5.4.2 Specific SOF Requirements - TOE

The specific required strength metrics for the functional components are given in Table 5-3.

Table 5-3 – SOF Metrics - TOE

#	CC Component	Name	Explicit SOF Metric
1	FAU_GEN.1	Audit data Generation	—
2	FAU_GEN.2	User Identity Generation	—
3	FAU_SAR.1	Audit Review	—
4	FAU_SAR.2	Restricted Audit Review	—
5	FAU_SAR.3	Selectable Audit Review	—
6	FAU_SEL.1	Selective Audit	—
7	FAU_STG.1	Protected audit trail storage	provide a hardware write-protected copy of audit trail
8	FAU_STG.3	Action in case of Possible Audit Data Loss	—
9	FDP_ACC.1	Subset Access Control	—
10	FDP_ACF.1	Security Attribute Based Access Control	—
11	FDP_DAU.1	Basic data authentication	—
12	FDP_ETC.1	Export of user data without security attributes	—
13	FDP_IFC.1	Subset information flow control	—
14	FDP_IFF.1	Simple security attributes	—
15	FDP_ITC.1	Import of user data without security attributes	—
16	FDP_ITT.1	Basic internal transfer protection	—
17	FDP_RIP.1	Subset Residual Information protection	applications will take advantage of OS supplied mechanisms
18	FDP_SDI.1	Stored data integrity monitoring	MD5 or equivalent checksums will be used for critical data elements
19	FDP_UCT.1	Basic data exchange confidentiality	support equivalent of 1024 bit key exchange and triple DES (as well as weaker values as required by import/export restrictions)

#	CC Component	Name	Explicit SOF Metric
20	FDP_UIT.1	Data exchange integrity	MD5 or equivalent checksums will be used
21	FIA_AFL.1	Authentication Failure Handling	—
22	FIA_ATD.1	User Attribute Definition	—
23	FIA_SOS.1	Verification of Secrets	—
24	FIA_SOS.2	TSF Generation of Secrets	—
25	FIA_UAU.1	Timing of authentication	—
26	FIA_UAU.5	Multiple authentication mechanisms	—
27	FIA_UAU.6	Re-authenticating	—
28	FIA_UAU.7	Protected authentication feedback	—
29	FIA_UID.1	Timing of identification	—
30	FIA_USB.1	User-Subject Binding	—
31	FMT_MOF.1	Management of security functions behavior	—
32	FMT_MSA.1	Management of security attributes	—
33	FMT_MSA.3	Static attribute initialization	—
34	FMT_MTD.1	Management of TSF data	include operating system access controls in controlling access to TSF critical data
35	FMT_SAE.1	Time-Limited Authorization	—
36	FMT_SMR.1	Security roles	—
37	FPT_AMT.1	Abstract Machine Testing	—
38	FPT_FLS.1	Failure with preservation of secure state	—
39	FPT_ITC.1	Inter-TSF Confidentiality During Transmission	support equivalent of 1024 bit key exchange and triple DES (as well as weaker values as required by import/export restrictions)
40	FPT_ITI.1	Inter-TSF detection of modification	MD5 or equivalent checksums will be used
41	FPT_ITT.1	Basic internal TSF data transfer protection	disclosure: support equivalent of 1024 bit key exchange and triple DES (as well as weaker values as required by import/export restrictions) modification: MD5 or equivalent checksums will be used
42	FPT_RCV.1	Manual Recovery	—

#	CC Component	Name	Explicit SOF Metric
43	FPT_RPL.1	Replay detection	—
44	FPT_RVM.1	Non-Bypassability of the TSP	—
45	FPT_SEP.1	TSF Domain Separation	use underlying hardware ring structure to separate, at a minimum, kernel space from application space
46	FPT_TDC.1	Inter-TSF basic TSF data consistency	—
47	FPT_TRC.1	Internal TSF consistency	—
48	FPT_TST.1	TSF Testing	MD5 or equivalent checksums will be used
49	FRU_RSA.1	Maximum quotas	—
50	FTA_LSA.1	Limitation on scope of selectable attributes	—
51	FTA_MCS.1	Basic limitation on multiple concurrent session	—
52	FTA_SSL.1	TSF-initiated session locking	—
53	FTA_SSL.2	User-initiated locking	—
54	FTA_SSL.3	TSF-initiated termination	—
55	FTA_TAB.1	Default TOE access banners	—
56	FTA_TAH.1	TOE access history	—
57	FTA_TSE.1	TOE session establishment	—
58	FTP_ITC.1	Inter-TSF trusted channel	—
59	FTP_TRP.1	Trusted path	—
60	FPT_CS2.1	TSF synchronization	—

5.4.3 Specific SOF Metrics - IT Environment

In a CS2 “compliant” PP, for each of the functional components listed in Table 5-2, the corresponding entry from Table 5-3 is moved into Table 5-4 below.

Table 5-4 – SOF Metrics - IT Environment

#	CC Component	Name	Explicit SOF Metric

6. ASSURANCE REQUIREMENTS

{Editorial note: The contents of EAL-CS2 is still an open issue. However, it is very likely that the final set of assurances will be selected from those given here.}

The assurance requirements for CS2 are met by an augmented EAL2 that is henceforth termed evaluation assurance level – CS2 (EAL-CS2). EAL-CS2 stresses assurance through vendor actions that are within the bounds of current best-commercial-practice. EAL-CS2 provides, primarily via review of vendor supplied evidence, independent confirmation that these actions have been competently performed. EAL-CS2 also includes the following independent, third-party analysis: (1) confirmation of system generation and installation procedures, (2) verification that the system security state is not misrepresented, (3) verification of a sample of the vendor functional testing, (4) searching for obvious vulnerabilities, and (5) independent functional testing.

The assurance components for EAL-CS2 are summarized in Table 6-1. Appendix C gives the details of these assurance components. Table 6-2 lists those components of EAL-CS2 that augment EAL2 from part 3 of the CC.

Table 6-1 – EAL-CS2 Assurance Components

Assurance Class	Component ID	Component Title
Configuration Management	ACM_CAP.3	Authorization controls
	ACM_SCP.2	Problem tracking CM Coverage
Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, Generation, and Start-up Procedures
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive High-Level Design
	ADV_RCR.1	Informal Correspondence Demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance Documents	AGD_ADM.1	Administrator Guidance
	AGD_USR.1	User Guidance
Life Cycle Support	ALC_DVS.1	Identification of Security Measures
	ALC_FLR.2	Flaw reporting procedures
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing - High-Level Design
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
Vulnerability Assessment	AVA_MSU.2	Validation of Analysis
	AVA_SOF.1	Strength of TOE Security Function Evaluation
	AVA_VLA.1	Developer vulnerability Analysis

Table 6-2 – EAL-CS2 augmentation to EAL-2

EAL2	CS2-EAL	Nature of Augmentation to EAL2
ACM_CAP.2	ACM_CAP.3	• requires a CM plan • describe how plan is used • provide evidence that – CM is operating in accordance with plan – configuration items are being effectively maintained – only authorized changes are made to configuration items
none	ACM_SCP.2	• CM documentation shows that CM system tracks – TOE implementation – design documentation – test documentation – user and administrator documentation – CM documentation – security flaws • CM documentation describes how configuration items are tracked
none	ADV_SPM.1	• provide an informal TOE security policy model that – describes rules and characteristics of all policies that can be modeled. – includes a rationale demonstrating consistency and completeness with respect to these policies • show consistency and completeness between all security functions in the functional specification and the model
none	ALC_DVS.1	• produce developmental security documentation that – describes the security measures necessary {in the opinion of the developer} to provide, for the TOE design and implementation, what confidentiality and integrity the developer considers necessary – provides evidence that these measures are being followed during TOE development and maintenance • evaluator confirms that the security measures identified are being applied Note: The evaluator does not, at ALC_DVS.1, confirm that the list of security measures in adequate. That is added at the next higher component (ALC_DVS.2).

EAL2	CS2-EAL	Nature of Augmentation to EAL2
none	ALC_FLR.2	• establish procedure for accepting and action upon user reports of security flaws • document flaw remediation procedures – describing procedures used to track security flaws – describing methods to provide flaw information, corrections, and guidance to users – requiring that description of and effect of flaw be provided – requiring that corrective actions be identified and correction status be provided – ensuring that reported flaws are corrected and corrections issued to users – providing safeguards that any corrections do not introduce new flaws
ATE_COV.1	ATE_COV.2	• requirement for developer analysis of test coverage – changing, for correspondence between test coverage and the functional specification, “evidence … show” to “analysis … demonstrate” • requirement that the coverage is ‘complete’
none	ATE_DPT.1	• requirement for developer analysis of test depth – depth sufficient to demonstrate operates in accordance with high-level design
none	AVA_MSU.2	• requirements placed upon guidance documentation – identify all possible modes of operation, their consequences and implications toward secure operation – be complete, clear, consistent, and reasonable – list all assumptions about the intended environment – list all requirements for external security measures • developer analysis of guidance documentation for completeness • evaluator confirmation of analysis of documentation completeness

7. APPLICATION NOTES

7.1 Evaluation Scope, Depth, and Rigor.

In lieu of extensive, independent analysis, CS2 intends the evaluator to:

a. Review developer supplied evidence to make a determination on:

   i) the competence of the vendor
   ii) the apparent correctness and completeness of the required security actions

b. Approach all requirements to ensure “all”, “any”, or “none” as generic CC requirements to be interpreted loosely when applied to this lower assurance evaluation.

c. Be consciously aware that there is a point at which more evaluation is not cost-effective; keeping in mind that CS2 is a lower assurance, lower cost, basic level of security.

This intention to limit independent analysis directly applies to the following assurance elements:

a. ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

b. ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

c. ADV_IND.2.2E The evaluator shall test the TSF to confirm that the TSF operates as specified.

d. AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

e. AVA_MSU.2.4E The evaluator shall confirm that the analysis shows that guidance is provided for secure operation in all modes of operation of the TOE.

f.

g. AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

h. AMA_CAT.1.2E The evaluator shall confirm that the categorization of TOE components and tools, and the categorization scheme used, are appropriate and consistent with the evaluation results for the certified version.

i.

8. RATIONALE

The rationale for this PP guidance is found in [CS2-R].

9. REFERENCES

[CC-V2] *Common Criteria for Information Technology Security Evaluation*, May 1998.

[CS2-R] *Rationale for CS2 - Protection Profile Guidance for Near-Term COTS*, version 0.4, date-TBD

APPENDIX A: ACRONYMS

CC	Common Criteria [for IT Security Evaluation]
COTS	Commercial Off The Shelf
EAL	Evaluation Assurance Level
IT	Information Technology
NIST	National Institute of Standards and Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

APPENDIX B: FUNCTIONAL REQUIREMENT DETAILS

Refinements used throughout functional elements:

1. ST Assignment: Where there is the potential for ST specific assignment -

- the following has been added to the PP assignment:

  "sufficient information for the ST author to make a compliant, ST specific assignment"

- and the following ST assignment has been added:

  [ST assignment: as [allowed | required] by PP, {ST specific assignment}]

The ST assignment may be "required" by the PP. This is where the PP author expects ST details to impact this requirement. An ST assignment may also be "allowed" by the PP. When "allowed", the PP author does not require that the ST add detail, but perceives that it may and wants to specify the requirements imposed on that detail. In either case (required or allowed), the PP author is expected to provide the detail necessary to enable evaluation of ST compliance with the PP. Examples of each case are:

Required. Identifying TSF data to be protected is an example of "required" ST assignment. The PP author may know general descriptions of TSF data, but need to have the ST author specify ST specific TSF data meeting PP defined criteria. For this particular example, it is anticipated that if the ST author chose to make a "null" assignment, then the ST would have to justify that there is no ST specific data meeting the PP criteria.

Allowed. An example of an allowed ST assignment is where the PP author provides a list of authorized roles, but is willing to allow the ST author to identify additional roles that may be unique to this ST and suitable for this requirement. In this case, the ST would probably not have to justify a "null" assignment, but would have to justify any additional roles as within the bounds specified by the PP. The ST author may wish to specify an additional role if having this role as authorized facilitates other requirements placed on the TOE.

2. ST Selection: A similar general refinement has been applied to the case of a potential ST selection. Here the initial PP choice may have been a selection or an assignment.

PP selection. Rather than selecting from CC choices, the PP author may choose to defer to the ST. For example, with FDP_RIP, the PP author may not care, at the PP level of abstraction, whether the mechanism performs before allocation or after deallocation. The PP might require that the ST explicitly state the choice made and justify that this choice is correct in light of the rest of the ST.

PP assignment. The PP author may choose to handle an assignment by generating a list of choices from which the ST author must select. An example of this is FAU_STG.3 where the PP author may generate a list of acceptable actions to be taken in the event of audit trail exhaustion. By letting the ST select from among allowable choices, the specific characteristics of the TOE can influence which action, or set of actions, is used.

Audit (fau)

FAU_GEN.1 Audit data generation

Dependencies: FPT_STM.1 (FPT_CS2.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events relevant for the [basic] level of audit; and

c) [***PP assignment:*** *other auditable events and sufficient information for ST author to make a compliant, ST specific assignment*]

d) [***ST assignment:*** *as required by the PP, other ST specific auditable events*]

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and [success, failure] of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***PP assignment:*** *other audit relevant information and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by the PP, other ST specific audit relevant information*].

Extension:

> FAU_GEN.1.3-CS2 When the TSF provides application support it shall support an application program interface that allows a privileged application to append data to the security audit trail or to an application-specified alternative security audit trail.

FAU_GEN.2 User identity generation

Dependencies: FAU_GEN.1, FIA_UID.1

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the individual identity of the user [***refinement:*** or system process] that caused the event.

Refinement: See text of FAU_GEN.2.1

FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1

FAU_SAR.1.1 The TSF shall provide [***PP assignment:*** *authorized users and sufficient information for ST author to make a compliant ST specific assignment*] and [***ST assignment:*** *as allowed by the PP, ST specific authorized users*] with the capability to read [***PP assignment:*** *list of audit information and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by the PP, list of audit information arising due to the specifics of the TOE design*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

FAU_SAR.2 Restricted audit review

Dependencies: FAU_SAR.1

FAU_SAR_2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

FAU_SAR.3 Selectable audit review

Dependencies: FAU_SAR.1

FAU_SAR.3.1 The TSF shall provide the ability to perform [searches, sorting, and ordering] of audit data based upon [***PP assignment:*** *multiple criteria with logical relations and sufficient information for the ST author to make a compliant, ST specific assignment*], [***ST assignment:*** *as allowed by PP, ST specific multiple criteria with logical relations*].

FAU_SEL.1 Selective audit

Dependencies: FAU_GEN.1
FMT_MTD.1

FAU_SEL.2.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) [Object identity, user identity, subject identity, host identity, and/or event type];
b) [***PP assignment:*** *list of additional attributes and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific additional attributes*] that audit selectivity is based upon.

FAU_SEL.2.2 The TSF shall provide only the [***PP assuagement:*** *authorized users and sufficient information for the ST author to a make compliant, ST specific assignment*] [***ST assignment:*** *as allowed by PP, ST specific authorized users*] with the ability to [select or display] which events are to be audited.

Extension:

FAU_SEL.2.3-CS2 The TSF shall provide the capability of FAU_SEL.2.2 at any time during the operation of the TOE.

FAU_STG.1 Protected audit trail storage

Dependencies: FAU_GEN.1

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to [prevent and detect] modifications to the audit records.

FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1

FAU_STG.3.1 The TSF shall take [***PP assignment:*** *actions to be taken in case of possible audit storage failure or list of acceptable actions from which the ST author can make a selection with requirements on how selection is to be performed*] [***ST selection:*** *as allowed by PP, from PP supplied list of actions*] if the audit trail exceeds [***refinement:*** an authorized user selectable, pre-defined limit].

Refinement:

See text in FAU_STG.3.1

User Data Protection (fdp)

FDP_ACC.1 Subset access control

Dependencies: FDP_ACF.1

FDP_ACC.1.1 The TSF shall enforce the [***PP assignment:*** *access control SFP*] on [***PP assignment:*** *list of subjects, objects, and operations among subjects and objects covered by the SFP and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific subjects, objects, and operations among subjects and objects covered by the SFP*].

FDP_ACF.1 Security attribute based access control

Dependencies: FDP_ACC.1, FMT_MSA.3

FDP_ACF.1.1 The TSF shall enforce the [***PP assignment:*** *access control SFP*] to objects based on [user identity, group membership,] [***PP assignment:*** *other security attributes and sufficient information for ST author to make a compliant, ST specific assignment*], and [***ST assignment:*** *as allowed by PP, other ST specific security attributes*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed [***PP assignment:*** *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***PP assignment*:** *rules, based on security attributes, that explicitly authorize access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***PP assignment:*** *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Extension:

> FDB_ACF.1.5-CS2 The TSF shall provide the capability to assign a user to be a member of more than one user group simultaneously.
>
> FDP_ACF.1.6-CS2 The TSF shall enforce the rules for authorizing and denying access based upon these precedence rules: [***PP assignment:*** *list of precedence rules for determining access or sufficient information on precedence needs for the ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as allowed by PP, ST specific precedence rules*].

Application note. Potential rules for controlling access include:

a) It shall be possible to permit or deny access for a specific user or group of users for a specific mode of access.

b) At least two modes of access, equivalent to read (observe) and write (modify) shall be defined.

c) It shall be possible to permit or deny access to public (or world) to apply in cases where no specific user or group identity applies

d) Precedence of rules:

1) If a mode of access is denied to a specific user identity, deny access.
2) If a mode of access is permitted to a specific user identity, permit access.
3) If a mode of access is denied to any group of which the user is a member, deny access
4) If a mode of access is permitted to any group of which the user is a member, grant access
5) If a mode of access is denied to public, deny access
6) If a mode of access is permitted to public, grant access
7) Else deny access.

FDP_DAU.1 Basic data authentication

Dependencies: None

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [***PP assignment:*** *list of objects or information types and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific objects or information types*].

FDP_DAU.1.2 The TSF shall provide [***PP assignment:*** *list of subjects and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific subjects*] with the ability to verify evidence of the validity of the indicated information.

FDP_ETC.1 Export of user data without security attributes

Dependencies: FDP_ACC.1 or- FDP_IFC.1

FDP_ETC.1.1 The TSF shall enforce the [***PP assignment:*** *access control SFP and/or information flow control SFP*] when exporting user data, controlled under the SFP, outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1

FDP_IFC.1.1 The TSF shall enforce the [***PP assignment:*** *information flow control SFP*] on [***PP assignment:*** *list of subjects, objects and operations among subjects and objects covered by the SFP and sufficient information for ST author to make a compliant, ST specific assignment*], and [***ST assignment:*** *as required by PP, list of ST specific subjects, objects and operations among subjects and objects covered by the SFP*].

FDP_IFF.1 Simple security attributes

Dependencies: FDP_IFC.1, FMT_MSA.3

FDP_IFF.1.1 The TSF shall enforce the [***PP assignment:*** *information flow control SFP*] to enforce at least the following types of subject and object security attributes [***PP assignment:*** *minimum number and type of security attributes and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, the ST specific minimum number and type of security attributes*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and a controlled information via a controlled operation if the following rules hold [***PP assignment:*** *for each operation, the security attribute-based relationship that must hold between subject and object security attributes and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, for each operation, any ST specific security attribute-based relationship that must hold between subject and object security attribute*].

FDP_IFF.1.3 The TSF shall enforce the [***PP assignment:*** *additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall enforce the following [***PP assignment:*** *list of additional SFP capabilities*].

FDP_IFF.1.5 The TSF shall explicitly authorize an information flow based on the following rules: [***PP assignment:*** *rules, based on security attributes, that explicitly authorize information flows*].

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [***PP assignment:*** *rules, based on security attributes, that explicitly deny information flows*].

FDP_ITC.1 Import of user data without security attributes

Dependencies: FDP_ACC.1 or/and FDP_IFC.1, FMT_MSA.3

FDP_ITC.1.1 The TSF shall enforce the [***PP assignment:*** *access control SFP and/or information flow control SFP*] when importing user data, controlled under the SFP, from outside the TSC.

FDP_ITC.1.2 The TSF shall ignore the security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following [***PP assignment:*** *additional importation control rules and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, any ST specific additional importation control rules*] when importing user data controlled under the SFP from outside the TSC.

FDP_ITT.1 Basic internal transfer protection

Dependencies: FDP_ACC.1 or/and FDP_IFC.1

FDP_ITT.1.1 The TSF shall enforce the [***PP assignment:*** *access control SFP and/or information flow control SFP*] to prevent the [***PP selection:*** *disclosure, modification, loss of use*] of user data when it is transmitted between physically-separated parts of the TOE.

FDP_RIP.1 Subset residual information protection

Dependencies: None

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***PP assignment:*** *allocation of the resource to, deallocation of the resource from or sufficient information to allow ST author to make a compliant selection*] [***ST selection:*** *as allowed by PP: allocation of the resource to, deallocation of the resource from*] the following objects [***PP assignment:*** *list of objects and sufficient information for ST author to make a compliant ST specific assignment*] and [***ST assignment:*** *as required by PP, ST specific list of objects*].

FDP_SDI.1 Stored data integrity monitoring

Dependencies: None

FDP_SDI.1.1 The TSF shall monitor user data stored within the TSC for [***PP assignment:*** *integrity errors and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as allowed by PP, ST specific integrity errors*] on all objects, based on the following [***PP assignment:*** *user data attributes and sufficient information for ST author to make a compliant ST specific assignment*] [***ST assignment:*** *as required by PP, ST specific user data attributes*].

FDP_UCT.1 Basic data exchange confidentiality

Dependencies: FTP_ITC.1 or FTP_TRP.1, FDP_ACC.1 or/and FDP_IFC.1

FDP_UCT.1.1 The TSF shall enforce the [***PP assignment:*** *access control SFP and/or information flow control SFP*] to be able to [transmit and receive] objects in a manner protected from unauthorized disclosure.

FDP_UIT.1 Data exchange integrity

Dependencies: FTP_ITC.1 or FTP_TRP.1, FDP_ACC.1 or/and FDP_IFC.1

FDP_UIT.1.1 The TSF shall enforce the [***PP assignment:*** *access control SFP and/or flow control SFP*] to be able to [transmit or receive] user data in a manner protected from [modification, deletion, insertion, or replay] errors.

FDP_UIT.1.2 The TSF shall be able to determine on receipt of user data, whether [modification, deletion, insertion, or replay] has occurred.

Identification and Authentication (FIA)

FIA_AFL.1 Authentication failure handling

Dependencies: FIA_UAU.1

FIA_AFL.1.1 The TSF shall detect when [an authorized user configurable number of] unsuccessful authentication attempts [***refinement:*** over an authorized user configurable length of time] occur related to [initial account login, re-authentication after initial login, and [***PP assignment:*** *list of other authentication events and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific authentication events*].

FAI_AFL.1.2 After the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [***PP assignment:*** *list of actions required or list of acceptable choices from which ST author may select along with any requirements imposed on this selection*] [***ST selection:*** *as allowed by PP, from PP author provided list of actions*].

Refinement: See text of FIA_AFL.1.1

FIA_ATD.1 User attribute definition

Dependencies: None

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [***PP assignment:*** *list of security attributes and sufficient information for a compliant ST assignment of ST specific attributes*] and [***ST assignment:*** *as required by PP, list of ST specific security attributes*].

FIA_SOS.1 Verification of secrets

Dependencies: None

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [***PP assignment****: a defined quality metric or sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as allowed by PP, a ST specific, defined quality metric*].

Application note. Potential elements for security quality metric related to passwords include:

a. Passwords shall not be reusable by the same user identifier for a period of time that can be set by an authorized user.

b. The TSF shall not indicate to the user if he/she has chosen a password already associated with another user.

c. The TSF shall, by default, prohibit the use of null passwords during normal operation.

d. The TSF shall provide an algorithm for ensuring the complexity of user-entered passwords that meets the following requirements:

i. Passwords shall meet a system-specifiable minimum length requirement. The default minimum length shall be eight characters.

ii. The password complexity-checking algorithm shall be modifiable by the TSF. The default algorithm shall require passwords to include at least one alphabetic character, one numeric character, and one special character.

iii. The TSF should provide a protected mechanism that allows systems to specify a list of excluded passwords (e.g., company acronyms, common surnames).

iv. The TSF should prevent users from selecting a password that matches any of those on the list of excluded passwords.

FIA_SOS.2 TSF generation of secrets

Dependencies: None

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet [***PP assignment****: a defined quality metric or sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as allowed by PP, a ST specific, defined quality metric*].

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for [***PP assignment****: list of TSF functions and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, a ST specific, list of TSF functions*].

Application note. Potential elements for security quality metric related to password generation include:

a. The password generation algorithm shall generate passwords that are easy to remember (i.e., pronounceable).

b. The TSF should give the user a choice of alternative passwords from which to choose.

c. Passwords shall be reasonably resistant to brute-force password guessing attacks.

d. If the ``alphabet" used by the password generation algorithm consists of syllables rather than characters, the security of the password shall not depend on the secrecy of the alphabet.

e. The generated sequence of passwords shall have the property of randomness (i.e., consecutive instances shall be uncorrelated and the sequences shall not display periodicity).

FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1

FIA_UAU.1.1 The TSF shall allow [***PP assignment:*** *list of TSF mediated actions and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, ST specific list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of the user.

FIA_UAU.5 Multiple authentication mechanisms

Dependencies: None

IA_UAU.5.1 The TSF shall provide [***PP assignment:*** *list of multiple authentication mechanisms or sufficient information for the ST author to make a complaint assignment*] [***ST assignment:*** *as allowed by PP, list of multiple authentication mechanisms*] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [***PP assignment:*** *sufficient information for the ST author to make a compliant assignment*] [***ST assignment:*** *as required by PP, rules describing how the multiple authentication mechanisms provide authentication*].

FIA_UAU.6 Re-authentication

Dependencies: None

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [re-establishing a session following session locking, request to change authentication secrets,] [***PP assignment:*** *list of other conditions under which re-authentication is required and sufficient information for ST author to make a compliant, ST specific assignment*], and [***ST assignment:*** *as required by PP, list of other, ST specific conditions under which re-authentication is required*].

FIA_UAU.7 Protected authentication feedback

Dependencies: FIA_UAU.1

FIA_UAU.7.1 The TSF shall only provide [no indication of success or failure and no clear-text display of any secret authenticator] to the user while the authentication is in progress.

FIA_UID.1 Timing of identification

Dependencies: None

FIA_UID.1.1 The TSF shall allow [***PP assignment:*** *list of TSF-mediated actions and sufficient information for ST author to make a compliant, ST specific assignment*] and [[***ST assignment:*** *as required by PP, list of ST specific, TSF-mediated actions*]on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1

FUA_USB.1.1 The TSF shall associated the appropriate user security attributes with subjects acting on behalf of that user.

Security management (fmt)

FMT_MOF.1 Management of security functions behavior

Dependencies: FMT_SMR.1

FMT_MOF.1.1 The TSF shall restrict the ability to [determine the behavior of, disable, enable, modify the behavior of] the functions [***PP assignment:*** *list of functions and potential modification and sufficient information for ST author to make a compliant assignment*] and [***ST assignment:*** *as required by PP, list of ST specific functions and potential modification*] to [***PP assignment:*** *the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as allowed by PP, the ST specific authorized identified roles*].

FMT_MSA.1 Management of security attributes

Dependencies: FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1

FMT_MSA.1.1 The TSF shall enforce the [***PP assignment:*** *access control SFP, information flow control SFP*] to restrict the ability to [change_default, modify, and delete] and [***PP selection:*** *read*] the values of the security attributes [***PP assignment:*** *list of security attributes and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific security attributes*] to [***PP assignment:*** *the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as allowed by PP, the ST specific authorized identified roles*].

FMT_MSA.3 Static attribute initialization

Dependencies: -FMT_MSA.1, FMT_SMR.1

FMT_MSA.3.1 The TSF shall enforce the [***PP assignment:*** *access control SFP, information flow control SFP*] to provide [***PP assignment:*** *restrictive, permissive, other property*] default values for object security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [data object owner and other authorized users] to specify alternate initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Dependencies: FMT_SMR.1

FMT_MTD.1.1 The TSF shall restrict the ability to [change_default, read, modify, delete, or clear] the [***PP assignment:*** *list of TSF data and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific TSF data*] to [***PP assignment:*** *the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as allowed by PP, the ST specific authorized identified roles*].

FMT_SAE.1 Time-limited authorization

Dependencies: FMT_SMR.1, FMT_STM.1 (FMT_CS2.1)

FMT_SAE.1.1 The TSF shall restrict the ability to specify an expiration time for [***PP assignment:*** *list of security attributes for which expiration is to be supported and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, list of ST specific security attributes for which expiration is to be supported*] to [***PP assignment:*** *the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as allowed by PP, the ST specific authorized identified roles*].

FMT_SAE.1.2 For each of these security attributes, TSF shall be able to [***PP assignment:*** *list of actions to be taken for each security attribute and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.

FMT_SMR.1 Security roles

Dependencies: FIA_UID.1

FMT_SMR.1.1 The TSF shall maintain the roles [**PP assignment:** the authorized identified roles and sufficient information for ST author to make a compliant, ST specific assignment] and [**ST assignment:** as allowed by PP, the ST specific authorized identified roles].

FMT_SMR.1.2 The TSF shall be able to associate users the roles.

Protection of Trusted Security (FPT)

FPT_AMT.1 Abstract machine testing

Dependencies: None

FPT_AMT.3.1 The TSF shall run a suite of tests [during initial start-up and at the request of an authorized user], [***PP selection:*** *periodically during normal operation*], [***PP assignment:*** *other conditions and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as allowed by PP, other, ST specific conditions*] to demonstrate the correct operation of the security functions provided by the abstract machine which underlies the TSF.

FPT_FLS.1 Failure with preservation of secure state

Dependencies: ADV_SPM.1

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [***PP assignment:*** *list of types of TSF failures and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific types of TSF failures*].

FPT_ITC.1 Inter-TSF confidentiality during transmission

Dependencies: None

FPT_ITC.1.1 The TSF shall protect [***refinement:*** [***PP assignment:*** *list of TSF data and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific TSF data*]] transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

Refinement: See text of FPT_ITC.1.1

FPT_ITI.1 Inter-TSF detection of modification

Dependencies: None

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of [***refinement:*** [***PP assignment:*** *list of TSF data and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific TSF data*]] data during transmission between TSF and a remote trusted IT product within the following metric: [***PP assignment****: a defined modification metric and sufficient information for ST author to make a compliant, ST specific assignment*], [***ST assignment:*** *as allowed by PP, a ST specific, defined modification metric*].

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of [***refinement:*** [***PP assignment:*** *list of TSF data and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as*

required by PP, list of ST specific TSF data]] transmitted between the TSF and a remote trusted IT product and perform [***PP assignment:*** *list of actions to be taken or list of acceptable choices from which ST author may select along with any requirements imposed on this selection*] [***ST selection:*** *as allowed by PP, from PP author provided list of actions*] if modifications are detected.

Refinement: See text in FPT_ITI.1.1 and FPT_ITI.1.2

FPT_ITT.1 Basic Internal TSF data transfer

Dependencies: None

FPT_ITT.1.1 The TSF shall protect TSF data from [***PP selection:*** *disclosure, modification*] and [***refinement: PP selection:*** *deletion, replay*] when it is transmitted between separate parts of the TOE.

Refinement: See text in FPT_ITT.1.1

FPT_RCV.1 Manual recovery

Dependencies: ADV_SPM.1, AGD_ADM.1, FPT_TST.1

FPT_RCV.1.1 After a failure or service discontinuity, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RPL.1 Replay detection

Dependencies: None

FPT_RPL.1.1 The TSF shall detect replay for the following entities [**PP assignment:** list of identified entities and sufficient information for ST author to make a compliant, ST specific assignment] [**ST assignment:** as required by PP, list of ST specific identified entities].

FPT_RPL.1.2 The TSF shall perform [***PP assignment:*** *list of actions to be taken or list of acceptable choices from which ST author may select along with any requirements imposed on this selection*] [***ST selection:*** *as allowed by PP, from PP author provided list of actions*] when replay is detected.

FPT_RVM.1 Non-bypassability of the TSP

Dependencies: None

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before any security-related action is allowed to proceed.

FPT_SEP.1 TSF domain separation

Dependencies: None

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_TDC.1 Inter-TSF basic TSF data consistency

Dependencies: None

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [***PP assignment:*** *list of TSF data types and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, list of ST specific TSF data types*] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [***PP assignment:*** *list of interpretation rules to be applied by the TSF and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, list of ST specific interpretation rules to be applied by the TSF*] when interpreting the TSF data from another trusted IT product.

Refinement - added element, clarifying intent:

FPT_TDC.1.3-CS2 The TSF shall support maintaining consistent [***PP assignment:*** *list of TSF data types and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, list of ST specific data types*] between this TSF and another trusted IT product.

FPT_TRC.1 Internal TSF consistency

Dependencies: FPT_ITT.1

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [***PP assignment:*** *list of SFs dependent on TSF data replication consistency*].

FPT_TST.1 TSF testing

Dependencies: FPT_AMT.1

FPT_TST.1.1 The TSF shall run a suite of self tests [during initial start-up and at the request of an authorized user] and [***PP selection:*** *periodically during normal operation*] and [***PP assignment:*** *list of other conditions at which self test should occur or list of acceptable choices from which ST author may select along with any requirements imposed on this selection*] [***ST selection:*** *as allowed by PP, from PP author provided list of actions*] to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of stored TSF executable code.

FPT_CS2.1 TSF synchronization

Non-CC component

Extension:

Not hierarchical to any other component.

Dependencies: None

FPT_CS2.1.1 The TSF shall provide the capability to synchronize distributed TSF elements and to associate audit event records produced by multiple TSF entities.

Application note: This component is similar to FPT_STM “Time stamps”, but calls out the synchronization requirement instead of a specifying a mechanism (i.e., reliable time stamps”) that could be used for that purpose.

Resource utilization (fru)

FRU_RSA.1 Maximum quotas

Dependencies: None

FRU_RSA.1.1 The TSF shall enforce quotas limiting the maximum quota of the following resources: [***PP assignment:*** *controlled resources and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, ST specific controlled resources*] that [an individual user, a defined group of users, or a subject] can use [***PP selection:*** *simultaneously, over a specified period of time*].

TOE Access (FTA)

FTA_LSA.1 Limitation on scope of selectable attributes

Dependencies: None

FTA_LSA.1.1 The TSF shall restrict the scope of the session security attributes [***PP assignment:*** *session security attributes and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, ST specific session security attributes*], based on [***PP assignment:*** *attributes and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, ST specific attributes*].

FTA_MCS.1 Basic limitation on multiple concurrent sessions

Dependencies: FIA_UID.1

FTA_MCS.1.1 The TSF shall [***refinement:*** enable an authorized user to select at TOE startup whether or not to] restrict the maximum number of concurrent sessions that belong to the same user [***refinement:*** and to select, if restricting is enabled, the maximum number of allowed sessions per user].

FTA_MCS.1.2 [***refinement:*** If the TOE is to restrict the maximum number of concurrent sessions,] the TSF shall enforce [***refinement:*** an authorized user selected maximum number of sessions] per user.

Refinement: See text in FTA_MCS.1.1 and FTA_MCS.1.2

FTA_SSL.1 TSF initiated session locking

Dependencies: FIA_UAU.1

FTA_SSL.1.1 The TSF shall lock an interactive session after [***refinement:*** an authorized user specified] time interval of user inactivity by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL1.2 The TSF shall require the following events to occur prior to unlocking the session: [user authentication].

Refinement: See text in FTA_SSL.1.1

FTA_SSL.2 User-initiated locking

Dependencies: FIA_UAU.1

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive sessions by:

a) clearing or over-writing display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other then unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [user authentication].

FTA_SSL.3 TSF-initiated termination

Dependencies: None

FTA_SSL.3.1 The TSF shall terminate an interactive session after [***refinement:*** an authorized user specified] time interval of user inactivity.

Refinement: See text in FTA_SSL.3.1

FTA_TAB.1 Default TOE access banners

Dependencies: None

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Extension:

FTA_TAB.1.2-CS2 The TSF shall provide the capability for an authorized user to specify and subsequently modify the contents of this warning message.

FTA_TAH.1 TOE access history

Dependencies: None

TA_TAH.1.1 Upon successful session establishment, the TSF shall display the [date, time, method, and location] of the last successful session establishment to the user.

FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [date, time, method, and location] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the user interface without giving the user an opportunity to review the information.

FTA_TSE.1 TOE session establishment

Dependencies: None

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [refinement: an authorized user specified] attributes [including user identity, port of entry, time of day, day of the week,] [***PP assignment:*** *list of other attributes and sufficient information for ST author to make a compliant, ST specific assignment*], and [***ST assignment:*** *as allowed by PP, ST specific attributes*].

Refinement: See text in FTA_TSE.1.1

trusted path/channels (FTP)

FTP_ITC.1 Inter-TSF trusted channel

Dependencies: None

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the [refinement: ***PP assignment:*** *list of data types and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, list of ST specific data types*]] channel data from modification and [refinement: ***PP assignment:*** *list of data types and sufficient information for ST author to make a compliant, ST*

specific assignment] and [***ST assignment:*** *as required by PP, list of ST specific data types*]] channel data from disclosure.

FTP_ITC.1.2 The TSF shall permit [***PP selection:*** *the TSF, the remote trusted IT product*] to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [***PP assignment:*** *list of functions for which a trusted channel is required and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, list of ST specific functions for which a trusted channel is required*].

Refinement: See text in FTP_ITC.1.1

FTP_TRP.1 Trusted path

Dependencies: None

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [remote] users that is logically distinct from other communications paths and provides assured identification of its end points and protection of the [refinement: ***PP assignment:*** *list of data types and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific data types*] communicated data from modification and [refinement: ***PP assignment:*** *list of data types and sufficient information for ST author to make a compliant, ST specific assignment*] and [***ST assignment:*** *as required by PP, list of ST specific data types*]] communicated data from disclosure.

FTP_TRP.1.2 The TSF shall permit [***PP selection:*** *the TSF, local users, remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [initial user authentication, user re-authentication, and] [***PP assignment:*** *list of other services for which trusted path is required and sufficient information for ST author to make a compliant, ST specific assignment*] [***ST assignment:*** *as required by PP, list of ST specific services for which a trusted path is required*].

Refinement: See text in FTP_TRP.1.1

Appendix C: ASSURANCE REQUIREMENT DETAILS

Configuration Management (ACM)

ACM_CAP.3 Authorization controls

Dependencies: CM_SCP.1, ALC_DVS.1

Developer action elements:

ACM_CAP.3.1D The developer shall provide a reference for the TOE.
ACM_CAP.3.2D The developer shall use a CM system.
ACM_CAP.3.3D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labeled with its reference.
ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.
ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.
ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the TOE configuration items.
ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.
ACM_CAP.3.7C The CM plan shall describe how the CM system is used.
ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.
ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.
ACM_CAP.3.10C The CM system shall provide measures such that only authorized changes are made to the configuration items.

Evaluator action elements:

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ACM_SCP.2 Problem tracking CM coverage

Dependencies: ACM_CAP.3

Developer action elements:

ACM_SCP.2.1D The developer shall provide CM documentation.

Content and presentation of evidence elements:

ACM_SCP.2.1C The CM documentation shall show that the CM system, as a minimum, tracks: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, CM documentation, and security flaws.
ACM_SCP.2.2C The CM documentation shall describe how configuration items are tracked by the CM system.

Evaluator action elements:

ACM_SCP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Delivery and operation (ADO)

Delivery and operation provides requirements for correct delivery, installation, generation, and start-up of the TOE.

ADO_DEL.1 Delivery procedures

Dependencies: None

Developer action elements:

ADO_DEL.1.1D The developer shall document the procedures for delivery of the TOE or parts of it to the user.
ADO_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation of evidence elements:

ADO_DEL.1.1C The delivery documentation shall describe the procedures which are necessary to maintain security when distributing versions of the TOE to a user site.

Evaluator action elements:

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1 Installation, generation, and start-up procedures

Dependencies: AGD_ADM.1

Developer action elements:

ADO_IGS.1.1D The developer shall document procedures to be used for the secure installation, generation, and start-up of the TOE.

Content and presentation of evidence elements:

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

Evaluator action elements:

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADO_IGS.1.2E The evaluator shall confirm that the installation procedures result in a secure configuration.

Development (ADV)

ADV_FSP.1 Informal functional specification

Dependencies: ADV_RCR.1

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

Content and presentation of evidence elements:

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.
ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.
ADV_FSP.1.4C The functional specification shall completely represent the TSF.

Evaluator action elements:

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

ADV_HLD.1 Descriptive high-level design

Dependencies: ADV_FSP.1, ADV_RCR.1

Developer action elements:

ADV_HLD.1.1D The developer shall provide the high-level design of the TSF.

Content and presentation of evidence elements:

ADV_HLD.1.1C The presentation of the high-level design shall be informal.
ADV_HLD.1.2C The high-level design shall be internally consistent.
ADV_HLD.1.3C The high-level design shall describe the structure of the TSF in terms of subsystems.
ADV_HLD.1.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.
ADV_HLD.1.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.
ADV_HLD.1.6C The high-level design shall identify the interfaces of the subsystems of the TSF.
ADV_HLD.1.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

Evaluator action elements:

ADV_HLD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_HLD.1.2E The evaluator shall determine that the high-level design is an accurate an complete instantiation of the TOE security functional requirements.

ADV_RCR.1 Informal Correspondence Demonstration

Dependencies: None

Developer action elements:

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

Content and presentation of evidence elements:

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

Evaluator action elements:

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_SPM.1 Informal TOE security policy model

Dependencies: ADV_FSP.1

Developer action elements:

ADV_SPM.1.1D The developer shall provide an TSP model.
ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

Content and presentation of evidence elements:

ADV_SPM.1.1C The TSP model shall be informal.
ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modeled.
ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modeled.
ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that there are no security functions in the functional specification are consistent and complete with respect to the TSP model.

Evaluator action elements:

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Guidance documents (AGD)

AGD_ADM.1 Administrator guidance

Dependencies: ADV_FSP.1

Developer action elements:

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

Content and presentation of evidence elements:

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE
AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.
AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.
AGD_ADM.1.4C The administrator guidance shall describe all security parameters under the control of the administrator indicating safe values as appropriate.
AGD_ADM.1.5C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_ADM.1.6C The administrator guidance shall be consistent with all other documents supplied for evaluation.
AGD_ADM.1.7C The administrator guidance shall describe all security requirements on the IT environment which are relevant to the administrator.

Evaluator action elements:

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_USR.1 User Guidance

Dependencies: ADV_FSP.1

Developer action elements:

AGD_USR.1.1D The developer shall provide user guidance.

Content and presentation of evidence elements:

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.
AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.
AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.
AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including all assumptions about user behavior found in the statement of TOE security environment.
AGD_USR.1.5C The user guidance shall be consistent with all other documentation delivered for evaluation.
AGD_USR.1.6C The user guidance shall describe all security requirements on the IT environment which are relevant to the user.

Evaluator action elements:

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Life Cycle Support (ALC)

ALC_DVS.1 Identification of security measures

Dependencies: None

Developer action elements:

ALC_DVS.1.1D The developer shall produce development security documentation.

Content and presentation of evidence elements:

ALC_DVS.1.1C The development security documentation shall describe the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.
ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

Evaluator action elements:

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_DVS.1.2E The evaluator shall check whether the security measures are being applied.

ALC_FLR.2 Flaw reporting procedures

Dependencies: None

Developer action elements:

ALC_FLR.2.1D The developer shall document the flaw remediation procedures.
ALC_FLR.2.2D The developer shall establish a procedure for accepting and acting upon user reports of security flaws and requests for corrections to those flaws.

Content and presentation of evidence elements:

ALC_FLR.2.1C The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2C The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3C The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4C The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
ALC_FLR.2.5C The procedures for processing reported security flaws shall ensure that any reported flaws are corrected and the correction issued to TOE users.
ALC_FLR.2.6C The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.

Evaluator Action Elements:

ALC_FLR.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Tests (ATE)

ATE_COV.2 – Analysis of coverage

Dependencies: ADV_FSP.1, ATE_FUN.1

Developer action elements:

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

Content and presentation of evidence elements:

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF as described in the functional specification and the tests identified in the test documentation is complete.

Evaluator Actions:

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_DPT.1 Testing: High Level Design

Dependencies: ADV_HLD.1, ATE_FUN.1

Developer action elements:

ATE_DPT.2.1D The developer shall provide the analysis of the depth of testing.

Content and presentation of evidence elements:

ATE_DPT.2.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TOE operates in accordance with the high level design.

Evaluator action elements:

ATE_DPT.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional Testing

Dependencies: None

Developer action elements:

ATE_FUN.1.1D The developer shall test the TSF and document the results.
ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation of evidence elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results.
ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.
ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.4C The test results in the test documentation shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each security function operates as specified.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent Testing - Sample

Dependencies: ADV_FSP.1, AGD_USR.1, AGD_ADM.1, ATE_FUN.1

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation of evidence elements:

ATE_IND.2.1C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2E The evaluator shall test the TSF to confirm that the TSF operates as specified.
ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

AVA_MSU.2 Validation of Analysis

Dependencies: ADO_IGS.1, AGD_ADM.1, AGD_USR.1, ADV_FSP.1

Developer action elements:

AVA_MSU.2.1D The developer shall provide guidance documentation.
AVA_MSU.2.2D The developer shall document an analysis of the guidance documentation.

Content and presentation of evidence elements:

AVA_MSU.2.1C The guidance documentation shall identify all possible modes of operation of the TOE, including operation following failure or operational error, their consequences and implications for maintaining secure operation.
AVA_MSU.2.2C The guidance documentation shall be complete, clear, consistent and reasonable.
AVA_MSU.2.3.C The guidance documentation shall list all assumptions about the intended environment.
AVA_MSU.2.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).
AVA_MSU.2.5C The developer's analysis documentation shall demonstrate that the guidance documentation is complete.

Evaluator action elements:

AVA_MSU.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_MSU.2.2E The evaluator shall repeat all configuration and installation procedures, and other procedures selectively, to check that the TOE can be configured and used securely using only the supplied guidance documentation.
AVA_MSU.2.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.
AVA_MSU.2.4E The evaluator shall confirm that the analysis shows that guidance is provided for secure operation in all modes of operation of the TOE.

AVA_SOF.1 Strength of TOE Security Function Evaluation

Dependencies: ADV_FSP.1, ADV_HLD.1

Developer action elements:

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each identified mechanism identified in the ST as having a strength of TOE security function claim.

Content and presentation of evidence elements:

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.
AVA_SOF.1.2C For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

Evaluator action elements:

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

AVA_VLA.1 Developer vulnerability analysis

Dependencies: ADV_FSP.1, ADV_HLD.1, AGD_ADM.1, AGD_USR.1

Developer action elements:

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP.
AVA_VLA.1.2D The developer shall document the disposition of identified vulnerabilities.

Content and presentation of evidence elements:

AVA_VLA.1.1C The evidence shall show, for each vulnerability, that the vulnerability cannot be exploited in the intended environment for the TOE.

Evaluator action elements:

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VLA.1.2E The evaluator shall conduct penetration testing, based on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

Maintenance of assurance (AMA)

None

APPENDIX 6. INFORMATION SYSTEMS SECURITY IN THE ACQUISITION PROCESS

APPENDIX 6.

INFORMATION SYSTEMS SECURITY IN THE ACQUISITION PROCESS

600. PURPOSE. Many FAA systems are procured in full or in part. To ensure that the appropriate security measures are built into the system or component, the acquisition process must address system security needs. This section describes the security activities performed throughout the acquisition process.

601. OVERVIEW OF MAJOR ACQUISITIONS. The FAA Acquisition Management System (AMS) defines the phases and key decision points of system acquisition and requires that security be considered at each point. The FAA's Acquisition Management System provides the framework for the FAA's Acquisition Cycle, which consists of five phases: Mission Analysis, Investment Analysis, Solution Implementation, In-Service Management, and Service Life Extension. Security activities related to information systems must be performed in all acquisitions. See Table 6-1 for a summary of security activities.

a. Mission Analysis Phase. Operational needs are the major area of focus during this phase. When an acquisition is planned, the ISS plan must be updated to reference the Mission Need Statement. Security threats and vulnerabilities shall be documented in the Mission Need Statement.

b. Investment Analysis Phase.

(1) Information is generated to determine the best overall solution to satisfy the mission need. For product or system acquisitions, this phase includes two major security activities:

(a) Specification of the security requirements. System planners define the system's security, which must be an integral part of the system requirements. These security requirements include both functional requirements (e.g., confidentiality, integrity, availability, and accountability) and assurance requirements (e.g., documentation, testing, security practices). The IS security level of the information to be used and protected by the system defines the minimum ISS requirements [see Chapter 2, section 2, and, Appendix 5]. These minimum requirements shall be modified, based on a review for adherence to policy, standards, and guidelines, and applicability and sufficiency for the intended operational environment. The information system security requirements are documented and maintained with ISS plan package. (See Chapter 4)

(b) Determination of security features, assurances, and operational practices. The system engineering team, including security engineers and user representatives, should work together to ensure that the features, assurances, and operational practices reflect the system's security needs. Security issues must be effectively addressed throughout the life cycle of the system, especially during the development phase. Security shall also be considered in feasibility studies, system cost-benefit analyses, software conversion studies, analysis of technical alternatives, and market surveys conducted during this phase.

(2) A copy of the ISS plan and supporting documentation must be provided to the ISS Division prior to the Acquisition Review so the ISS Division can advise the Joint Resources Council (JRC) whether the plan should be approved.

(3) The risk management process is used to support decision-making in this phase. The Investment Analysis Phase risk analysis is performed prior to the approval of design specifications consistent with OMB Circular A-130. Risk management drives the selection of appropriate, cost-effective safeguards and forms the basis for determining mandatory and desirable specifications. Risk management is further discussed in Chapter 2, section 3.

(4) To ensure continuity throughout the system life cycle, the DAA shall be assigned for new systems early in this phase and shall participate in security-related decisions concerning the acquisition. For system acquisitions, the line of business shall establish a security working group to address security issues related to the system procurement, contractor selection, guidance and oversight of the development effort, product acquisition, acceptance support, operational assurance, testing and eventual decommissioning of the system. This group's members will be drawn from or integrated into the Integrated Product Team (IPT) as well as any additional members whose expertise may be beneficial.

Table 6-1. Security Activities during the Acquisition Cycle for Major Systems

AMS Phases	*Security Activities*
Mission Analysis	• Identify unique needs of the information systems (IS). • Document security needs, threats, and vulnerabilities in the Mission Need Statement and include this information in the ISS plan. • Preliminarily assess the sensitivity of the information to be protected by the IS. • Determine the need for IS confidentiality, integrity, availability, and accountability.
Investment Analysis	• Assign in writing the DAA and provide a copy of the designation letter to the ISS Division. • Establish a security working group to address security issues related to procurement, contractor selection, and system development. • Specify IS security requirements: -functional requirements (confidentiality, integrity, availability, and accountability). -assurance requirements (documentation, security testing, security procedures, etc) -minimum security requirements definition • Determine adherence to line of business and agency security policy and standards. • Determine sufficiency of the ISS plan for the intended operational environment, and adjust plan, if necessary. • Integrate planned security into overall system design and development plans, cost-benefit analysis, and other pertinent studies and analyses. • Provide a copy of the ISS plan to the ISS Division or SSE. • Perform risk analysis and select cost-effective safeguards before IS design specifications are approved.
Solution Implementation	• Specify security in the Statement of Work (SOW) and include in Screening Information Request (SIR) and ISS, if applicable. • Require potential contractors to show that they have documented processes for implementing security within a product, system, or service and for supporting ISS certification and authorization activities. • Determine if potential contractors will be required to demonstrate competency in implementing security in their development processes by achieving SSE-CMM level 1. • Security working group reviews SOW to ensure adequate security is addressed. • Include security in the system test program. • Contractor appoints individual responsible for implementing security. • Contractor develops a security assurance package. • SSE reviews SIR. • State IS security level and relevant requirements in SOW. • Disqualify contractors who do not meet security requirements. • Ensure adequate background investigations on critical personnel. • Verify implementation of security requirements in system. • Monitor COTS for compliance with security requirements. • Test system's security features. • Certifying authority (CA) conducts certification testing.
In-Service Management	• Configure provided security features. • Provide training on security administration and secure operations. • Actively monitor sources of information regarding threats and vulnerabilities. • Triennial compliance review by ISSC.
Service Life Extension	• Include new security requirements as needed.

c. Solution Implementation Phase.

(1) The system is acquired, developed, and integrated during this phase. Security activities start with the specification of security in the Statement of Work (SOW). The SOW shall be contained in the Screening Information Request (SIR) and shall be included in the ISS plan package. The IPT security working group must ensure that the SOW includes provisions requiring potential contractors to demonstrate that they have documented processes for implementing security within a product or system and for supporting the system's certification and

authorization activities. Potential contractors may be required to demonstrate their competency in implementing security in their development processes. They can show this ability by achieving an industry-standard System Security Engineering Capability Maturity Model (SSE-CMM) rating of at least capability level 1 (performed informally) in all of the technical security process areas or an agreed-upon subset.

(2) The SOW shall contain all information system security requirements to be required of the winning contractor. Therefore, the security working group shall review the SOW to ensure that security needs are adequately addressed. Each information system security requirement in the SOW shall be annotated as required or desired. Failure to respond adequately to the required items is grounds for disqualifying the offeror. Failure to respond adequately to the desired items is grounds for subtracting evaluation points.

(3) SOW authors shall consider security as integral to all components of the architecture, including the network, telecommunications, hardware, software, and database. For developmental acquisitions, the authors shall integrate security requirements with system reliability and availability requirements, and with operational requirements to aid in selecting products and technology that address security.

(4) The SOW must include security as a key element of the system test program. The contractor shall be tasked to appoint an individual who shall be responsible for implementing the system's technical security and who shall represent the contractor as a member of the security working group throughout the remainder of the acquisition and implementation process.

(5) The SOW shall require the contractor to participate in certification and authorization activities including, but not limited to, creating an assurance package to support the security implementation of the system being developed. The assurance package must include security documentation as specified in the Contract Data Requirements List (minimally, a discussion of the security design, security test documentation, a security administration manual, and a security guide for system users) and a discussion of the developmental assurances used by the contractor during the development effort. The components of this package must be approved by the DAA and the contents shall be included in the ISS plan package and provided as attachments for the authorization of the system.

(6) Ensure that appropriate technical, administrative, physical, and personnel security requirements are included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services. For FAA-wide procurements, the ISS Division must review and approve the SIR to ensure that security needs are appropriately specified. For local or regional procurements, review and approval of the SIR shall be performed by the SSE.

(7) The SOW shall specify the following:

(a) Rules of conduct that a contractor shall be required to follow.

(b) List of the anticipated threats and hazards (technical, physical, and personnel) that the contractor must guard against.

(c) Description of the safeguards that the contractor must specifically provide.

(d) Information system security standards applicable to the contract.

(e) Description of the test methods, procedures, criteria, and inspection system needed to verify and monitor the safeguards during contract performance and to discover and counter any new threats or hazards.

(f) Description of the procedures for conducting a formal risk assessment.

(g) Description of the personnel security requirements.

(h) Description of the security training that the contractor is required to provide to its employees and FAA employees. This training must be consistent with the guidelines for Federal information system security training issued by NIST and regulations issued by the OPM.

(i) Description of the plan that the contractor must develop or follow to provide for the security and privacy of information systems which the contractor is required to operate.

(8) The SOW shall indicate the security level of the information system being acquired. The security level is based on the mission and on the security level of the information to be used or produced by the information system. The security requirements shall be determined based on the security level of the information system and the corresponding protection needed as specified in Appendix 5.

(9) The proposal review team should include information system security personnel from outside the developing, procuring or owning organization. The proposal review team should be the same personnel who participated in developing the SOW. Their function is to evaluate whether the contractor's proposal meets the information system security requirements of the SIR and the SOW. An unsatisfactory response to information security requirements in the SOW and SIR is grounds for disqualifying the contractor.

(10) Threats that are active during this phase can introduce vulnerabilities to the technology. Assurances, such as background checks for system developers, code walkthroughs, testing, and design and documentation reviews, site surveys by ISS Division or regional personnel, shall be required by the SOW and can help minimize the risk during this phase.

(11) All system components are either procured off-the-shelf or designed and developed during this phase. The components are tested, integrated, tested again, and then installed. During this phase, the Information System Security Plan and the security engineering documentation are used to guide the information systems security aspects of testing, design and documentation reviews, and site surveys. The IPT shall periodically review development activities to ensure that the security aspects of the system are addressed and verified. Decisions concerning security shall be documented in the ISS plan and in supporting documentation. These documents are provided to the ISS Division, which shall advise the JRC on the acceptability of the ISS plan at each significant stage of the system's life cycle.

(12) For those parts of the system that are acquired off-the-shelf, security activities may include monitoring to ensure that security is a part of market surveys, contract solicitation documents, and evaluation of proposed systems. The security policies and implementations of COTS components are often incompatible with custom-developed components and other COTS products. Security integration requires considerable effort and shall be closely monitored by the IPT to ensure that the resulting system meets security specifications.

(13) The evaluation and testing of the system security includes the overall evaluation of the information system's security features, testing of the particular parts of the system that have been developed or acquired, and testing of the entire system. Security testing is performed at all levels of test, including unit test, integration test, and system test. Security testing is performed against the security requirements specified for the unit, element, or system under test.

(14) The SOW shall stipulate that the system shall undergo security testing and evaluation (ST&E) that must be approved by the ISS Division. According to the SOW, the IPT shall specify the development of an assurance package to support the formal authorization for system operation. The DAA shall review the documentation provided in the package to aid in determining whether adequate security safeguards have mitigated the risk to an acceptable level .

d. In-Service Management Phase.

(1) When acquired, most off-the-shelf systems come with security features disabled. These features must be enabled, configured, and tested. Custom-developed systems may also require configuration of security features, depending on the findings of the risk assessment and analysis.

(2) The SOW may require the contractor to provide system training sessions at the operational installations. If such training is required, the sessions shall include training on security administration and secure operations of the system.

e. Service Life Extension Phase. This phase of a system occurs when new requirements or changes to the environment cause the acquisition cycle to be reinitiated. Examples of Service Life Extension include instances of refreshing the technology and adding new capabilities. Recognition of new requirements causes the acquisition cycle to be reentered at the Mission Analysis or the Investment Analysis phase. ISS activities for service life extension acquisitions parallel those for new systems. Although many existing contracts do not contain sufficient security requirements or security solutions, opportunities for adding security features will arise in this phase when

additions and modifications to incumbent contracts occur. Contracting and project officers must negotiate reasonable timeframes to allow existing contractors to comply with this Order.

602. ACQUISITION OF SECURITY SERVICES. When the FAA decides to obtain supplementary support for security services, the acquisition process shall accommodate this need. These services shall be documented in a Mission Need Statement. In the Investment Analysis Phase, an SOW shall be prepared to detail the requirements to be satisfied by the provider of security services. Potential bidders shall demonstrate a documented process for providing the services specified in the SOW. Potential service providers may be required to demonstrate their competency by an SSE-CMM rating of at least capability level 1 (performed informally) for each process area covering the desired security services.

603. OVERVIEW OF OTHER ACQUISITIONS.

a. Initiation. Before purchase of products that are not considered a major acquisition, define operational needs, which is the major area of focus during this phase. Any unique security needs for information systems must be identified and included in the project definition. A preliminary assessment of the sensitivity of information to be protected by the system must be performed. Additionally, security objectives shall be assessed, including, at minimum, the need for confidentiality, integrity, availability, and accountability. This assessment shall consider legal implications, Federal policy, FAA policy, the functional needs of the system, and the importance of the system to FAA mission. When an acquisition is planned, the ISS plan must be updated to reference the project definition. Security threats and vulnerabilities shall be documented in the ISS plan as indicated in paragraph b of this paragraph. Appropriate appointments of ISS security managers and officers must be accomplished early in the cycle to ensure proper implementation of security requirements.

b. Definition. All acquisitions will have risk assessments completed and included in the security plan package. Once the initial ISS risk assessment is completed, subsequent risk assessments are conducted based on a system's progression through the acquisition and software completion processes. Focusing on the major vulnerabilities discovered through risk assessment will save resources. Documentation is attached to the initial ISS risk assessment and becomes a permanent part of the security plan package, resulting in a baseline for risk assessments conducted during the remainder of the life cycle. Acquisition of additional or upgraded components (hardware or software) covered by the ISS plan do not require a separate formal risk assessment unless a major change occurs that will affect security.

c. Design. After the ISS risk assessment is completed and appropriate safeguards are selected, those safeguards need to be effectively implemented. Subsequent ISS risk assessments will be conducted during all testing phases and in anticipation of major system or physical environment changes.

d. Development. Technical safeguards are not always feasible because of expense or interference with the system's reliability. The lack of feasibility must be documented to include the rationale, possible alternatives and the residual, acceptable risk that is assumed by the DAA. Explanations of the affect of the security features on a system will be included in the risk assessment. Personnel and physical security measures taken to augment technical safeguards will be documented in ISS risk assessments.

e. Test and Evaluation. All test results and evaluations will be included as part of the security plan package. Any vulnerabilities discovered during testing and subsequent safeguards will be recorded in the ISS risk assessment. See Chapter 10, Security Test and Evaluation.

f. Operations. When acquired, most off-the-shelf systems come with security features disabled. These features must be enabled, configured, and tested. Custom-developed systems will also require configuration of security features. The SOW may require the contractor to provide system training sessions at the operational installations for FAA personnel. If such training is required, the sessions shall include training on security administration and secure operations of the system.

APPENDIX 7. PHYSICAL SECURITY

APPENDIX 7.

PHYSICAL SECURITY FOR INFORMATION SYSTEMS

700. GENERAL. This appendix adopts physical security standards that are not addressed in FAA Order 1600.6, Physical Security Management Program. This appendix shall be used in addition to FAA Order 1600.6 and FAA Order 4650.21, Management and Control of In-Use Personal Property. The scope of this Appendix is the same as Chapter 1, paragraph 4 of this Order.

701. SITE SELECTION CRITERIA. Site selection is a key factor in the establishment and maintenance of a secure operating environment. The physical characteristics of any location selected to house FAA IS must support the establishment of a physical security system at the facility. Architectural design is an equally important aspect of the site selection and security relationship. The following points shall be considered in the site selection process:

a. Below ground level installations or other locations possibly subject to flooding shall be avoided.

b. Windows shall be avoided in IS equipment rooms because of their inherent vulnerability to forcible entry, the loss of usable floor space, and problems associated with solar heating. If the network, server or telecommunications area are located against an exterior building wall, adequate protection shall be provided against security intrusion, fire, storm, and explosion.

c. It is recommended that the equipment room be located in the center of the building. This ensures additional protection provided by the building.

d. Physical provisions for restricting access shall be incorporated into the initial design.

e. The existence or absence of activities above, below, or immediately adjacent to projected automation areas that might pose a hazard shall be considered.

f. Provide protection for critical areas as addressed in FAA Order 1600.6 and this Appendix.

g. Network equipment should be installed in areas located where danger from fire, smoke, and explosion is minimal. A thorough survey should be conducted prior to site selection to identify potential threats to the equipment.

h. A factor to be considered for the selection of a building structural design is resistance to the effects of hurricanes, earthquakes, tornadoes, high winds, electrical storms, etc.

i. IS equipment shall be protected by such normal and extra measures as required by providing overhead waterproofing, floor drains, pumps, alarms, emergency waterproof covers, etc., in accordance with Federal, state and local fire protection and building codes.

j. Any electronic device that produces, transmits or stores an electronic signal (i.e. IS, telecommunications equipment, etc.) are vulnerable to having these signals intercepted by electronic means. Individual rooms can be shielded to minimize the danger of this type of intercept, but it is important to ensure that heating/cooling ducts and electrical lines to these rooms are also shielded. Rooms can also be shielded to minimize audio or acoustic surveillance.

702. BUILDING. The physical security of IS depends to a large extent upon the adequacy of the construction of the structure in which it is housed. All structures will comply with applicable building codes (GSA, state or local) and fire codes (NFPA, GSA, state, local).

703. IS AREA ACCESS CONTROLS. Access controls are required to prevent unauthorized entry to an IS area and to control the flow of materials into and out of a facility. Positive access controls will be maintained at all times to IS areas. This shall be accomplished through, but are not limited to, the following means:

a. Designation as a Restricted Area. Each IS area designated a critical area (See FAA Order 1600.6, Chapter 6) shall be designated and posted as a **"RESTRICTED AREA"** (e.g., server room, telecommunications support area, Enterprise Network Operations Center (ENOC), areas housing gateways, backbones or firewalls).

b. Control of Personnel Access During Operational Hours. Appropriate positive security controls shall be implemented to assure that only authorized persons are permitted to enter the area. This shall be achieved by one or more of the following controls:

(1) maintaining a personnel access list

(2) physical barriers, such as counters, locked doors equipped with electrical/electronic release, mechanical cipher locks, closed circuit television, receptionist, badge system, etc.

(3) a buffer or control zone be created immediately outside of the primary entrance to the equipment room

(4) use of secondary or emergency entrances will be strictly controlled and monitored

c. Control of Personnel Access During Non operational Hours. All dedicated IS areas shall be secured upon the completion of the business day or at any other time when the area is unoccupied, such as during a fire drill, bomb threat, etc. Strict accountability shall be maintained over keys, key cards, cipher lock combinations, biometric files, or any other access devices. A comprehensive facility risk assessment conducted by the SSE may also disclose vulnerabilities in the after hours environment.

d. Visitor Control. Positive controls shall be implemented in each FAA IS area so that only authorized personnel are afforded unrestricted access. Appropriate visitor screening procedures shall be instituted to assure that other personnel permitted to enter the area do so only after their identity and requirement for access have been verified by proper authority. Visitors shall be escorted by authorized personnel.

704. PROTECTION OF OTHER ESSENTIAL OR CRITICAL AREAS. The following areas are listed as critical areas in accordance with FAA Order 1600.6. These work areas or support utility closets require physical security protection because of their importance to IS operations, because they represent or contain sensitive data or valuable assets, or because unrestricted access significantly increases the threat to the confidentiality, integrity, and security of data and applications software. The following areas shall be included in an IS or physical security risk assessment and meet with controls described in paragraph 703 of this Appendix:

a. Data storage and IS security libraries

b. Remote input/output areas

c. Data conversion area

d. Programmers' area and files

e. Documentation files

f. Communications equipment area

g. IS maintenance area

h. Off-site storage areas for back-ups to source code and operational software

i. Network areas

j. IS operations areas (e.g., server, backbone, gateways, firewalls)

k. Utility room or closets

l. Telephone closets

m. IS supplies storage

705. SECURITY OF DATA STORAGE AND IS SECURITY LIBRARIES. Areas used as storage locations for magnetic tapes, disc packs, CDs, back-up data media, IS security libraries (See Chapter 4 of this Order) shall have physical controls in accordance with paragraph 703 of this Appendix and any additional controls mandated by FAA Order 1600.6:

Additional security for media storage areas include:

(1) Access Controls. Personnel access to media storage areas or containers shall be positively controlled by appropriate physical and procedural measures. Highly sensitive data (e.g., FOUO, SSI) shall be further protected in locked storage cabinets (See Chapter 7 of this Order and FAA Order 1600.2). One person within a facility or area will be designated in writing as the media librarian and be accountable for contents of the library.

(2) After hour Protection. During periods when the IS area is not operational or when reduced staffing does not permit effective supervision to be maintained, the door to library areas or cabinets which contain sensitive or proprietary data shall be secured.

706. SECURITY OF REMOTE WORKSTATIONS. Some IS operations require use of remote access. Remote workstations, whether PC or laptop, have more potential for abuse, damage, theft, and unauthorized use than workstations located in a staffed FAA facility. Frequently, however, a remote workstation must be located in an area where the basic physical security principles and requirements of FAA Order 1600.6 and this Order cannot be applied easily.

FAA remotely accessed information systems are required to have the capability of disabling or disconnecting, either physically or by software, any or all of the remote workstations attached to the system. However, to assure adequate security at a remote site, the following additional procedures shall be applied:

a. Physical Control.

(1) Secured Area Concept. Where it is possible, a remote workstation shall be located in an area which is locked when not attended by an authorized user.

(2) Unsecured or Partially Secured Area Concept. If a lockable room is not available, the workstation shall be equipped with a disabling device and shall be disabled when not attended by an authorized user. Examples of physical disabling include power disconnect locks or keyboard locks with properly controlled key systems. In addition, consideration should be given to protecting the workstation from theft.

b. Administrative Control. Positive administrative safeguards shall be effected to assure that only authorized individuals are permitted to utilize remote IS equipment capable of accessing FAA information systems. Appropriate caution shall be exercised to assure that sensitive information displayed on the screen is not viewed by unauthorized personnel, and that hard or soft copy output containing sensitive information is received and removed from the IS area only by authorized individuals.

707. PROTECTION OF LAPTOPS, NOTEBOOKS AND OTHER PORTABLE EQUIPMENT. Because of the convenience of portability and opportunity for use in uncontrolled areas, FAA employees and contractors must take special care to assure proper use and protection of portable equipment. This equipment shall be used only in an area or in such a manner that FAA data will not be exposed to unauthorized individuals. This equipment shall be stored in controlled space, secured when not in use. Removal of this equipment from a building is subject to property removal controls. In addition, a checkout log shall be maintained for this equipment which shows to whom the equipment is checked out, purpose for which its outside use is authorized, date and time of removal, and date and time of return. Users under these conditions shall assure that sensitive data and authenticators are not compromised

by such use. Use of access script files that include user IDs and passwords for convenience of use is prohibited. See Chapter 5 and paragraph 708 of this Appendix for requirements for warning banners and markings.

708. SIGNAGE, EQUIPMENT MARKINGS AND WARNING BANNERS. Warning signs, markings and warning banners on and in U.S. Government facilities and equipment are required for successful prosecution for unauthorized access and use. With the introduction of COTS and service contracts for both administrative, NAS systems, and other operational systems, expansion of the signage rule is necessary to encompass non-FAA facilities as defined in Appendix A of FAA Order 1600.6.

a. FAA facilities. These facilities will apply warning signs, equipment markings and warning banners in accordance with FAA Order 1600.6, FAA Order 4650.21, Management and Control of In-Use Personal Property, and this Order.

b. Non-FAA facilities. These facilities shall post signage, markings and warning banners as indicated in this Order in the IS areas and on IS equipment that is owned by, or leased to, or used for the U.S. Government. The requirement to post signage, markings and warning banners shall be included in any contracts, statements of work (SOW), memoranda of understanding (MOU) or agreement (MOA), international agreements or other applicable documents.

(1) Non-government facilities. The following signage, markings or warning banners apply to these type of facilities (See Appendix A of FAA Order 1600.6 for definition):

(a) Restricted area signs. See paragraph 703 of this Appendix.

(b) Equipment markings. All IS equipment owned by, leased to, or used for the U.S. Government will be marked in a visible, permanent, legible manner with the words, **"Property of U.S. Government. Unauthorized access or use will be prosecuted under Federal law."**

(c) Warning banners. Electronic warning banners will be displayed in accordance with Chapter 5 of this Order.

(d) NAS warning signs. If an applicable IS area has data or equipment that relates to the NAS, a legible sign with the following terminology will be visibly placed in the applicable area:

> **"WARNING: This area is used in FAA Air Traffic Control. Loss of human life may result from service interruption. Any person who interferes with this system or gains unauthorized access into this area to commit damage, disruption or otherwise interfere with the FAA National Air Space System will be prosecuted under Federal law."**

The term "Air Traffic Control" is used in this warning banner because of its' recognition and association by the public at large.

(2) Government facilities. The following signage, markings or banners (or equivalents) apply to these type of facilities:

(a) Restricted area signs. See paragraph 704 of this Appendix.

(b) Equipment markings. All IS equipment owned by, leased to, or used for the U.S. Government, no matter where physically located, will be marked in a visible, permanent, legible manner with the words, **"Property of U.S. Government. Unauthorized access or use will be prosecuted under Federal law."**

(c) Warning banners. Electronic warning banners will be displayed in accordance with Chapter 5 of this Order.

(d) NAS warning signs. If an applicable IS area has data or equipment that relates to the NAS, a legible sign with the following terminology will be visibly placed in the applicable area:

"WARNING: This area is used in FAA Air Traffic Control. Loss of human life may result from service interruption. Any person who interferes with this system or gains unauthorized access into this area to commit damage, disruption or otherwise interfere with the FAA National Air Space System will be prosecuted under Federal law."

The term "Air Traffic Control" is used in this warning banner because of its' recognition and association by the public at large.

(e) If the IS area is located in a location under foreign control, substitute the phrase **"….under Federal law"** with **"….under International Agreements".**

709. SECURITY OF SOURCE CODE, OPERATIONAL SOFTWARE AND RELATED DOCUMENTATION. Master copies of source code, operational software and related documentation shall be placed in secure, fire-resistant storage areas or containers located in a secure off-site area. Additional master copies may be maintained in other regions or centers. Documentation files should be accorded adequate protection to prevent deliberate or inadvertent destruction, damage, or loss.

710. IS FILE AND RECORD PROTECTION. Back-ups and secure off-site storage shall be utilized as the primary method of safeguarding IS files and records. Physical security controls in this Appendix and FAA Order 1600.6 shall be used to protect the back-ups.

APPENDIX 8. MARKING OF FOUO AND SSI

APPENDIX 8.

MARKING OF FOUO AND SSI

800. PROTECTION OF INFORMATION MARKED FOR OFFICIAL USE ONLY.

a. Security levels CS1, CS2, and CS3 (see Table 2-3 or Appendix 5) identify information that is to be protected against uncontrolled release. FOR OFFICIAL USE ONLY is not a classification term (i.e., denoting national security information). It denotes unclassified information that requires protection against indiscriminate handling. Additional information is provided and referenced in FAA Order 1600.2 (limited distribution), paragraphs 642 and 643, and Appendix 10 which is available through the SSE.

b. Media containing information that requires protection against uncontrolled release shall be marked FOR OFFICIAL USE ONLY when necessary to ensure that all persons with access to the information are aware of the required protection. The marking FOR OFFICIAL USE ONLY shall include, in smaller print, the following notation: "Public availability to be determined under 5 U.S.C. 552." When printed, such markings shall be placed at the bottom of the outer cover, if any, on the first page, and on each succeeding page that contains FOUO information. When the media is computer-readable, such markings shall be placed in human-readable form on the outside of the media container. Markings, in the same format as the information, shall be placed on the first page or equivalent of the contained information and on each succeeding page or equivalent that contains FOUO information.

c. FAA Order 1600.2 specifies different requirements for storing FOUO items, depending on whether guards control access to the building or area. The Order directs that higher degrees of protection be used, depending on the sensitivity of the information, the time, or circumstances. Physical and technical means may be used either alone or in combination to provide higher degrees of protection.

d. FOUO information of any security level may not be transmitted, processed, or stored in any information system unless the system is authorized by its cognizant DAA to handle that security level.

801. SENSITIVE SECURITY INFORMATION (SSI). Records and information specified in 49 U.S.C. 40119 and 14 CFR Part 191 are not available for public inspection or copying, nor is information contained in those records released to the public. The information that may not be released may include, but is not limited to, documents containing references to system or facility vulnerabilities, risk, safeguards, security testing and evaluation (ST&E), inspection results, system development relating to security activities, contingency plans and any other documents or data that refers to system or facility security within the FAA. For a complete list of other types of information covered, see 49 USC 40119 and 14 CFR 191.7.

802. MARKINGS FOR SSI. An electronic document containing SSI shall have the protective marking, "**SENSITIVE SECURITY INFORMATION"**, applied to the top of each page. The distribution limitation in this paragraph shall be affixed to the bottom of each page.

a. Responsibility. The originator of information or records containing SSI shall in accordance with this section assign a protective marking that clearly identifies the information or records as SSI and specifies the distribution limitation required.

b. Requirements for Protective Marking. Any paragraph containing SSI material shall be marked "(SSI)" at the beginning of the paragraph. Any title, subject line, photograph, chart, graph, or figure that is within a document and that contains SSI shall also be marked "(SSI)". Each page containing SSI material shall have the protective marking applied to the top and bottom.

(1) Single page. The protective marking shall consist of the words **"SENSITIVE SECURITY INFORMATION"** stamped or printed in bold face capital letters that are larger than the other type on the page.

(2) Document with multiple pages. If the document consists of more than one page, in addition to the requirement for marking each page containing SSI the protective marking shall also be applied at the top and bottom of the outside of the front cover (if there is one), on the title page, on the first page, and on the outside of the back page or cover.

(3) Bound document. For a bound document the protective marking shall be applied in accordance with the requirements of paragraph 802. That is to say that each page in the document that contains SSI will have the protective marking applied as required by paragraph 803. In addition, the protective marking shall be applied to the outside front cover, the title page, the first page, and on the outside of the back page or cover as required by paragraph 802.

c. Requirements for Application of Distribution Limitation Statement. Whenever the protective marking "**SENSITIVE SECURITY INFORMATION"** is applied to any portion of a document or record, each page or surface containing the protective marking shall have the distribution limitation statement specified in this paragraph, stamped or typed on the bottom of the page or surface below the protective marking using bold face type and, if possible, a contrasting font at least as large as the print on the page. The distribution limitation statement that must be affixed to the bottom of each page immediately under the "**SENSITIVE SECURITY INFORMATION**" protective marking shall be as follows:

"WARNING: THIS DOCUMENT CONTAINS SENSITIVE SECURITY INFORMATION THAT IS CONTROLLED UNDER THE PROVISIONS OF 14 CFR PART 191. THE INFORMATION MAY NOT BE RELEASED IN ANY FORM WITHOUT THE EXPRESS PRIOR WRITTEN CONSENT OF THE ADMINISTRATOR OR ASSOCIATE ADMINISTRATOR FOR CIVIL AVIATION SECURITY, ACS-1. IN ACCORDANCE WITH 49 U.S.C. 40119, THIS INFORMATION IS EXEMPT BY STATUTE FROM DISCLOSURE UNDER THE FOIA. UNDER THE PROVISIONS OF 14 CFR PART 191.5(D), VIOLATORS ARE SUBJECT TO CIVIL PENALTY OR OTHER ACTION BY THE FAA."

(1) Single page. When a single page has been assigned the SSI protective marking, the distribution limitation statement shall be affixed to the bottom of the page below the protective marking.

(2) Document with multiple pages. When a document or record consists of multiple pages, the distribution limitation statement is required on the bottom of each page or record portion that has been assigned a protective marking as required by paragraph 802. This includes the cover page (if present), the title page, the first page, and the outside of the back page or cover.

(3) Bound document. The distribution limitation statement shall be affixed to the bottom of each page containing SSI and to the bottom of the front cover, the bottom of the title page, the bottom of the first page, and the bottom of the outside of the back page or cover.

d. Protective Markings for Charts, Maps, and Drawing. Charts, maps, and drawings shall have the appropriate protective markings and distribution limitation statement affixed in a manner that is plainly visible.

e. Protective Markings of Motion Picture Films and Video Recordings. The protective marking and distribution limitation statement shall be applied at the beginning and end of each reel. The protective marking and distribution limitation statement shall be affixed in such a manner that both are fully visible on the screen or monitor.

(1) Motion picture reels that are kept in film cans or other containers shall have protective markings and distribution limitation statements. The protective marking and distribution limitation statement shall be applied to each side of each reel and to all sides of each can or other storage container. In addition to reproducing the protective marking and distribution limitation on the beginning and end portions of the film if the motion picture has a soundtrack, audible warnings that describe the protective marking and distribution limitation shall, if possible, be included in the introduction and at the end of the film.

(2) Videotape recordings that contain SSI shall include on the recordings conspicuous visual protective markings and distribution limitation statements at both the beginning and the end. Protective markings and the distribution limitation statement shall also be applied on the front and back and on each side of the video case and storage containers.

f. Protective Marking and Distribution Limitation Statement on Information Extracted from Electronic Media. The protective markings and distribution limitation statement may be applied by the equipment itself on the face of the page provided the markings and distribution limitation statement are clearly distinguishable

from the printed text. Information and records in the form of compiled lists shall have the protective marking affixed to the top and bottom of the first and last pages, to the top and bottom of any covers, to the top and bottom of each page containing SSI, and to the outside of the back page or cover. The distribution limitation statement shall be affixed on the bottom of each page containing protective markings as required by paragraph 802.

g. Transmittal Documents. Documents that are used to transmit SSI material but do not themselves contain SSI shall be marked as required for SSI documents. In addition, the following statement shall be affixed to the front page of the transmittal document. A sample cover sheet may be found in Appendix 3 or is available electronically from the SSE.

> **"The protective marking SENSITIVE SECURITY INFORMATION and the distribution limitation statement on this document are canceled when the attachments containing SSI are removed."**

803. MAILING OR CONVEYANCE OF SSI. When assembling a package containing SSI for mailing or conveyance, it is the responsibility of the individual preparing the package to ensure that all SSI contains the appropriate protective markings and distribution limitation statements.

a. SSI material may be mailed outside an activity by U.S. Postal Service first class mail. SSI that is to be sent by mail shall be in a single opaque envelope, wrapping, or carton.

b. Within an activity, SSI shall be mailed or conveyed in a sealed envelope in such a manner as to preclude its unauthorized disclosure.

804. ELECTRONIC TRANSMISSION OF SSI. When transmitting SSI over FAA cc:mail, the following procedures shall apply :

a. The SSI information shall be transmitted in a password-protected attachment.

b. No electronic mail transmission shall be routed through a commercial Internet Service provider unless by protected by an encryption product from FIPS 140-1. See Chapter 6, par 601.

805. STORAGE OF SSI. All individuals possessing SSI are responsible for ensuring that the information and records are safeguarded at all times from disclosure to unauthorized personnel. When the SSI and records for which an individual is responsible are not under his or her direct control, the individual shall ensure that they are safeguarded and protected in such a way that they are not physically or visually accessible to persons who do not have a need to know. At a minimum, password protection should be utilized.

806. DESTRUCTION OF SSI. When material containing SSI is no longer needed, it shall be promptly and completely destroyed so that recovery of the SSI from the residue will be difficult or impossible. Destruction methods include burning, pulping or crosscut shredding or tearing into small pieces that shall be mixed with other waste paper material in the process. Reusable electronic media must be overwritten or degaussed. Contact the SSE for guidance on degaussing.